Administrators Guide

Clavister® FineTune™ Version 8.81

Administrators Guide
Clavister® FineTune™
Version 8.81

Published 2007-02-09
Build: 881

Copyright © 2007 Clavister AB.

Copyright Notice

Disclaimer

The information in this document is subject to change without notice. The manufacturer makes no representations or warranties with respect to the contents hereof and specifically disclaim any implied warranties of merchantability or fitness for any particular purpose. The manufacturer reserves the right to revise this publication and to make changes from time to time in the content hereof without obligation of the manufacturer to notify any person of such revision or changes.

Limitations of Liability

Table of Contents

List of Figures

List of Tables

List of Examples

Preface

Target Audience

The target audience for this publication is the administrator of a security gateway running the CorePlus operating system. The system may be running on Clavister hardware or non-Clavister hardware and is to be administered from a management workstation running the Clavister FineTune software.

Text Structure

The text is divided into chapters and subsections. Numbered subsections are shown in the table of contents at the beginning of the document.

Text links

Where a "See section" link is provided in the main text, this can be clicked on to take the reader directly to that reference eg. see Section 2.6, "Gateways".

Web links

Web links included in the document are clickable eg. http://www.clavister.com.

Notes to the main text

Special sections of text which the reader should pay special attention to are indicated by icons on the the left hand side of the page followed by a short paragraph in italicized text. There are the following types of such sections:

Note
This indicates some piece of information that is an addition to the preceding text. It may concern something that is being emphasised or something that is not obvious or explicitly stated in the preceding text.

Caution
This indicates where the reader should be careful with their actions as an undesirable situation may result if care is not exercised.

Important
This is an essential point that the reader should read and understand.

Warning
This is essential reading for the user as they should be aware that a serious situation may result if certain actions are taken or not taken.

Chapter 1. Getting Started

1.1. Installing FineTune

Clavister Security Gateways are configured and monitored from a software management tool called FineTune, designed to run on a server or workstation running Microsoft Windows with TCP/IP network access to the gateways. This server or workstation will be also be referred to as the *management station*.

The complete FineTune software can be found on the CD-ROM included with the delivered Clavister hardware. This should be used to install FineTune on a Microsoft Windows based PC. The recommended minimum PC configuration is:

- Microsoft Windows 2000 or later

- 128 MBytes RAM

- 50 Mbytes free hard disk space

- A network card

Insert the included CD-ROM into the CD-ROM drive of the Windows PC. If the installation software does not start automatically, select **Run** from the **Start** menu and enter D:\launch.exe (where D: is the letter of your CD-ROM drive).

You will be presented with a list of options. Select the option to install the FineTune software.

1.2. Adding new Gateways

This section describes how to enable management of a Clavister Security Gateway by FineTune. It is assumed that the Clavister Security Gateway has been installed, that the base configuration has been performed according to the *Installation and Setup* guide, and finally that the selected management interface on the Clavister Security Gateway is connected to a network reachable from the management station running FineTune

Running the New Security Gateway wizard

Start the FineTune software from the **Start** menu and follow these steps:

1. The first time FineTune is started (and only the first time) the following dialog will appear. Move your mouse over the dialog until the progress bar is filled. This generates a random number which will be used for encryption of communication between FineTune and Clavister Security Gateways.
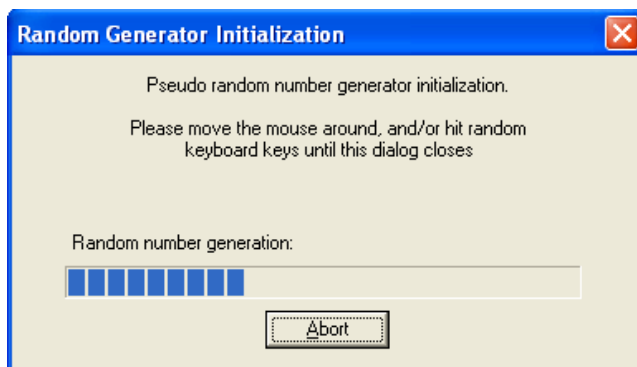
2. The FineTune interface will now be visible on the screen. Click the **Security Editor** icon in the left toolbar or select it from the **Tools** menu.

   The first time the security editor is started (and only the first time) you will see following dialog next. This will ask if you wish to import a "Default" gateway configuration. This is recommended for the new user as this can be used as a basis for setting up a customized configuration.
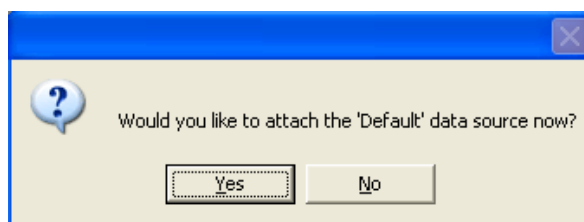
   This same dialog will then appear again asking if you wish to import "Samples" which are a set of example gateway configurations. This is also recommended for the new user.

3. Locate and select the **Security Gateways** folder, then start the New Security Gateway Wizard by clicking the **New** icon in the toolbar.
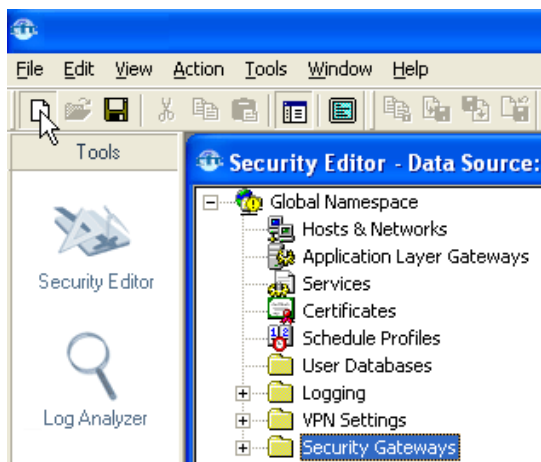
4. Select **Appliance** or **Software** or **Custom** in the wizard depending on your product type. If you are using Clavister hardware you should select **Appliance**. If you are using non-Clavister hardware then **Software** should be selected. Click **Next** to continue.

5. Enter a descriptive name and the IP address of the Clavister Security Gateway. The IP address is used to communicate with the gateway from FineTune. (In most cases this is the IP address you entered during installation and set up of the hardware). Click **Next** to continue.

Note
Remember this IP address, as you will need to enter it again in the Clavister Security Gateway console.

6. Now choose a password for the local console access. Leave the password blank if there is no demand for local console protection. Click **Next** to continue.

> *Note*
> *This password is used for local console access only, and is in no way related to the way FineTune authenticates with the Clavister Security Gateway.*

7. *(Non-Clavister hardware only).* The supplied Clavister CD-ROM which contains all software, can be used as a bootable media. However it is advisable to also create a backup to this on a burnable CD-ROM. Using the smaller *mini-core* (marked as *mini* in the list), it is also possible to create a bootable floppy disk.

   Select the device to use for creation of the alternative boot media for the hardware from the list displayed. Make sure the selected type is available.

   Click **Next** to continue.

8. *(Non-Clavister hardware only)* Select a core to be installed on the Clavister Security Gateway. Click **Next** to continue.
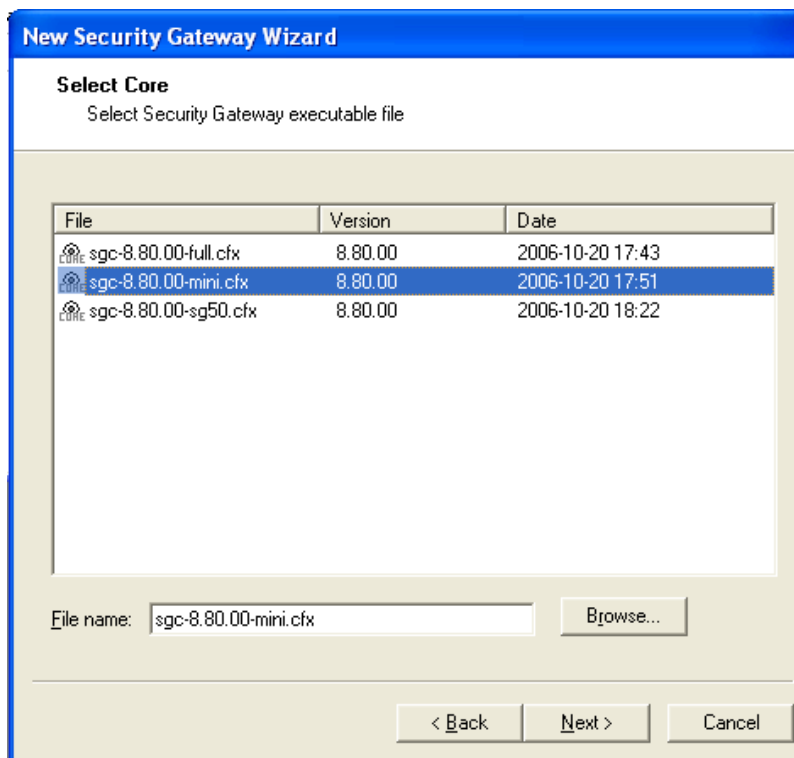
9. *(Non-Clavister hardware only)* The wizard will now write all necessary files to the boot media. You can examine the process in detail by clicking the **Properties...**button. When the boot media creation is finished, click **Next** to continue.
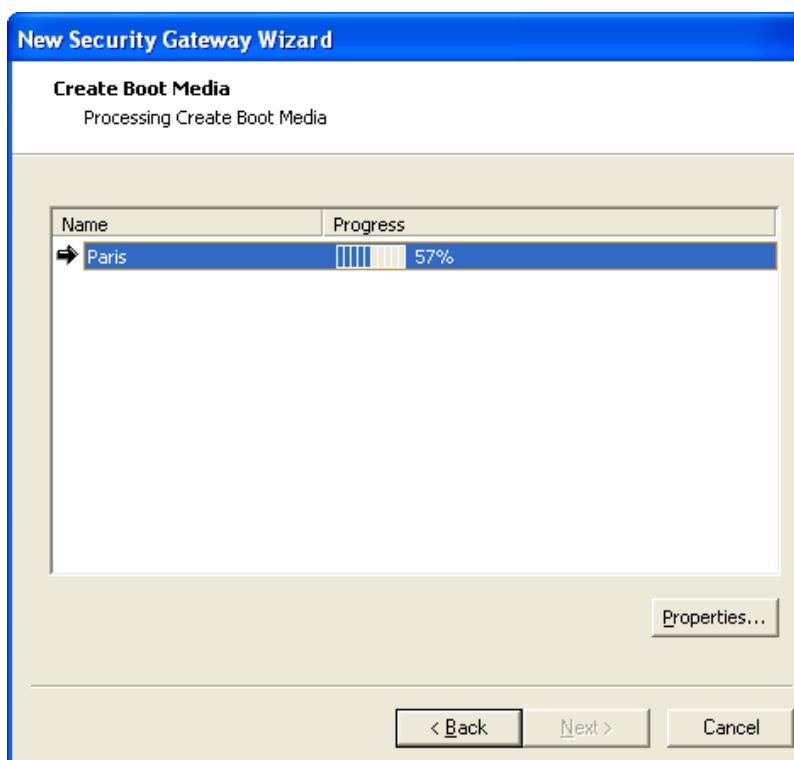
10. *(Non-Clavister hardware only)* Remove the boot media and insert it into to your gateway hardware.
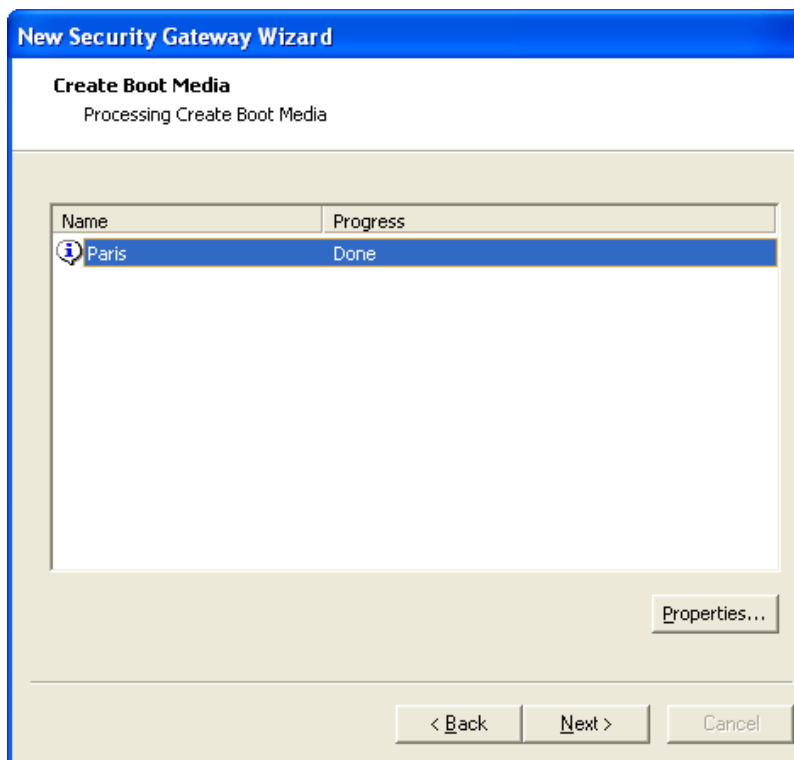
11. The wizard will now try to connect to the Clavister Security Gateway. It will remain in this state until a successful connection is made or **Cancel** is selected.
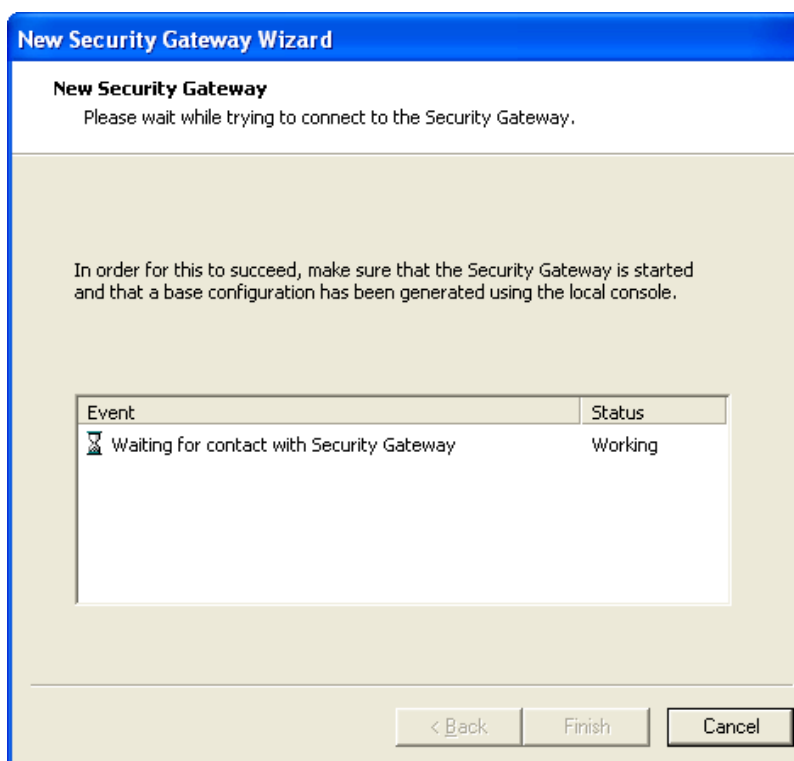
12. If everything is working correctly, the management station should now begin to communicate with the Clavister Security Gateway. During this process the management station will download the running configuration, exchange new encryption keys for remote management and set the local console password if enabled.
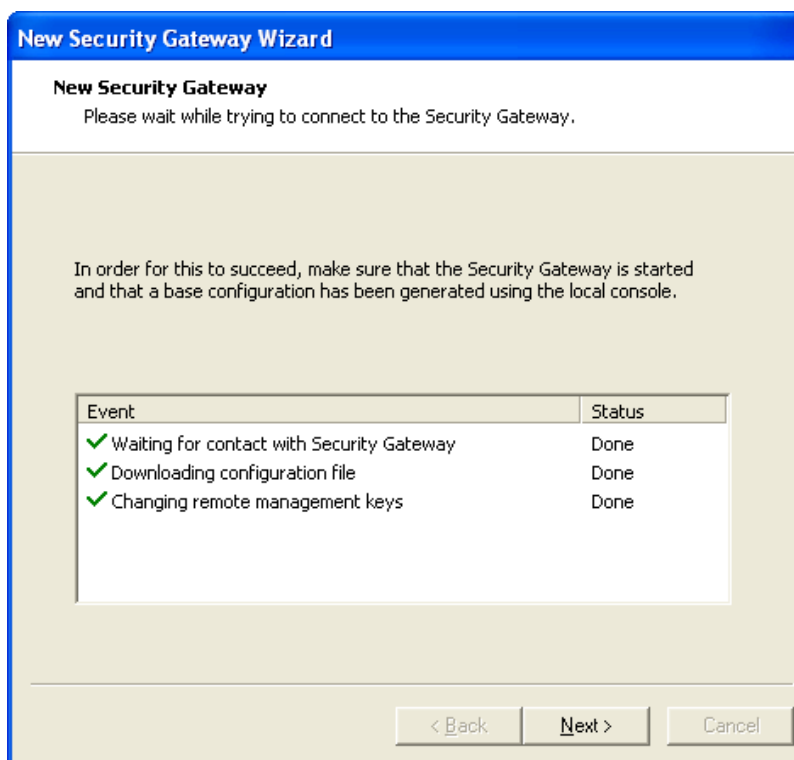
If an error occurs or the manager fails to connect to the Clavister Security Gateway, please read Appendix A, *Troubleshooting a new gateway*.

13. Finally the wizard will collect information about DNS servers, time zone and daylight settings. To accomplish DNS resolving please enter one or more DNS servers. Furthermore, enter appropriate time zone settings. These settings can be set later on but preferably you do this now. Click **Finish**.
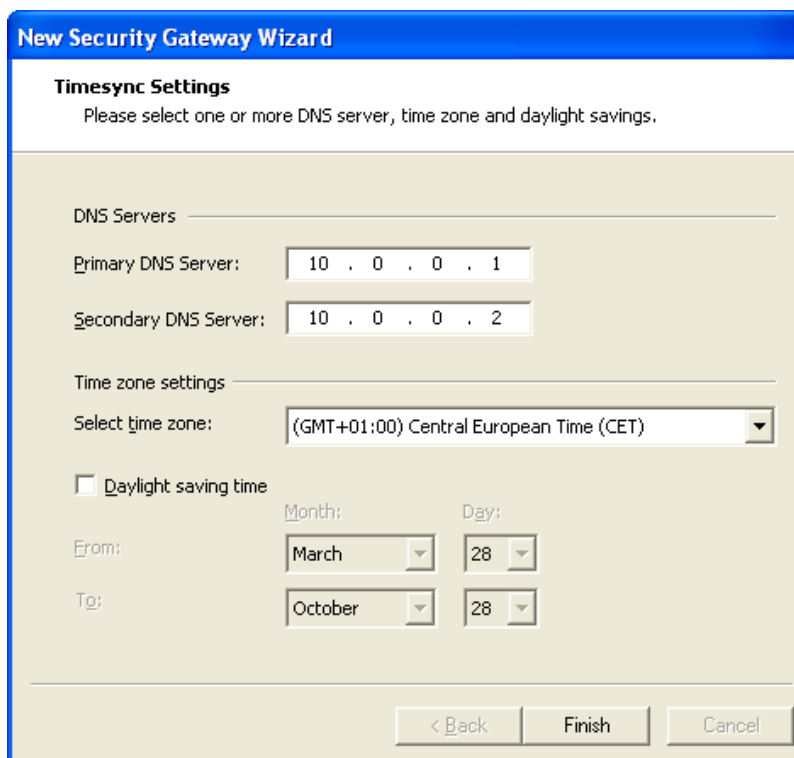
Congratulations, your Clavister Security Gateway is now up and running and configured with a small base configuration!

The next steps include registering the Clavister license and modifing your first security policy using FineTune.

1.3. Registering a Clavister license

A Clavister license can be retrieved by using the *Registration wizard*. The wizard is automatically launched immediately after the *New Security Gateway Wizard* has been completed. The wizard can also be started at a later time by first selecting the Clavister Security Gateway target for the registration, and then choose **Register...** from the **Action > License** menu in the Security Editor.

There are two registration options, one for new users, and one for existing users.
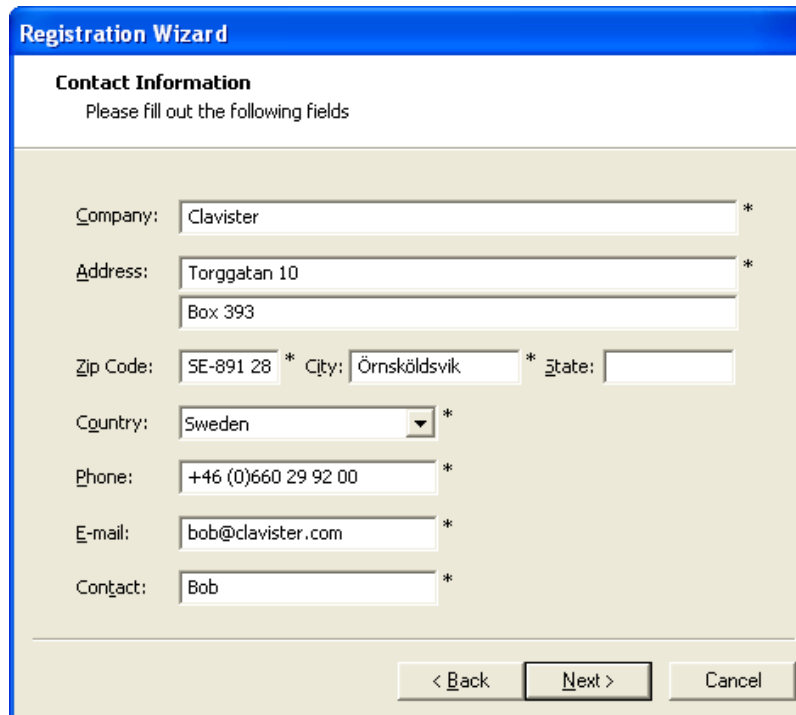
The first option, called **First-time User**, should be chosen for new users who have not yet registered any products with Clavister. The user will then be asked to enter registration details, and to choose a username and password, which is required to access the Clavister Client Web.

For existing users, who have previously registered one or more products with Clavister, the second option, called **Existing User**, should be chosen. For this option skip to Section 1.3.2, "Existing user".
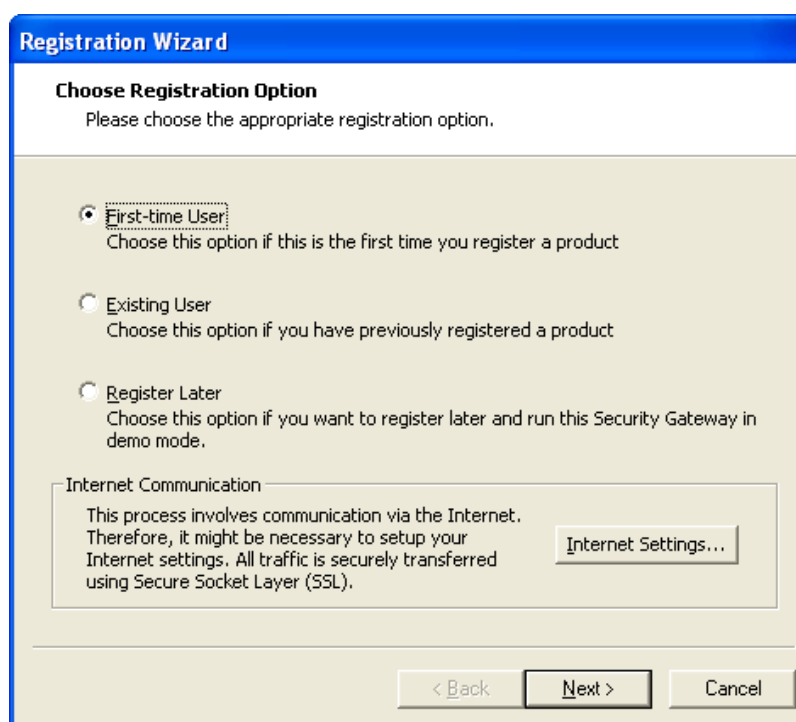
1.3.1. First time user

1. Registration details are entered here. Fields marked with an asterisk (*) are necessary fields and must be filled in.
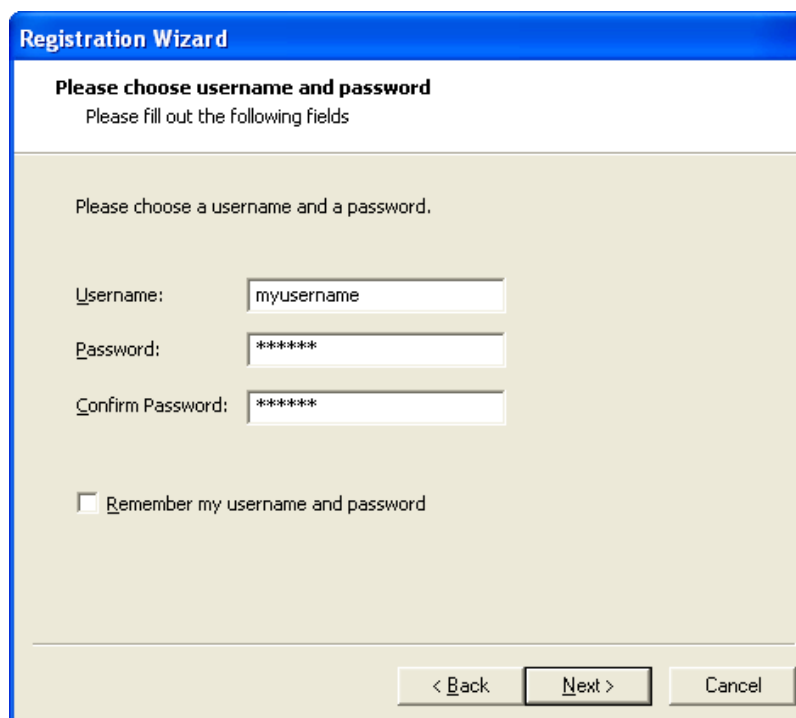
2. To simplify future access to the Clavister Client Web, a username and password has to be chosen. This will be used for actions related to licenses, such as visiting the Clavister Client Web via a browser, or downloading an updated license file via Clavister FineTune.

Note that Clavister FineTune can save the username and password in the Windows Registry. If so, the next time an operation is performed that requires the Clavister Client Web username and password, this will not be prompted for. This is however a security risk, as both username and password is stored in plaintext.

> *Note*
> *The username and password must still be entered manually if visiting the Clavister Client Web via a browser.*

3. Clavister Security Gateway hardware product packaging includes a *Certificate of Authenticity*. On this certificate, a registration key is printed. The registration key is formatted as four groups, with each group containing four digits.

   The registration key should be entered here. This key will be used, together with other registration information, to create a valid license file.
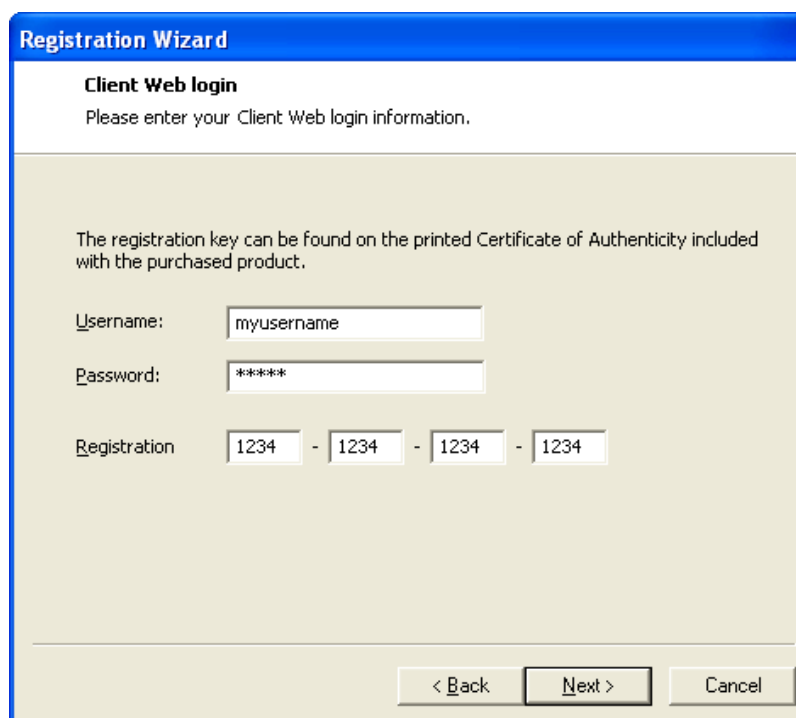
   A new user should skip the next section and go to Section 1.3.3, "Registering continued"

1.3.2. Existing user

In order to connect to the Clavister Client Web, the username and password chosen the first time the user registered with Clavister must be entered here.

The registration key, as found on the *Certificate of Authenticity*, which is included in the Clavister Security Gateway product package, must also be entered here. The registration key is formatted as four groups, with each group containing four digits.

If the username and password has previously been saved in the Windows Registry, Clavister Security Gateway will automatically fill in those fields.

1.3.3. Registering continued

1.   *(Non-Clavister hardware only)* In order to create a unique license file for each user, a license will always be bound to the MAC address of one of the Ethernet adapters in the Clavister Security Gateway.

     If FineTune is able to communicate with the Clavister Security Gateway, a list of all available Ethernet adapters, along with their MAC addresses, will be presented.

     If FineTune fails to connect to the Clavister Security Gateway, the MAC address of the Ethernet adapter has to be entered manually.
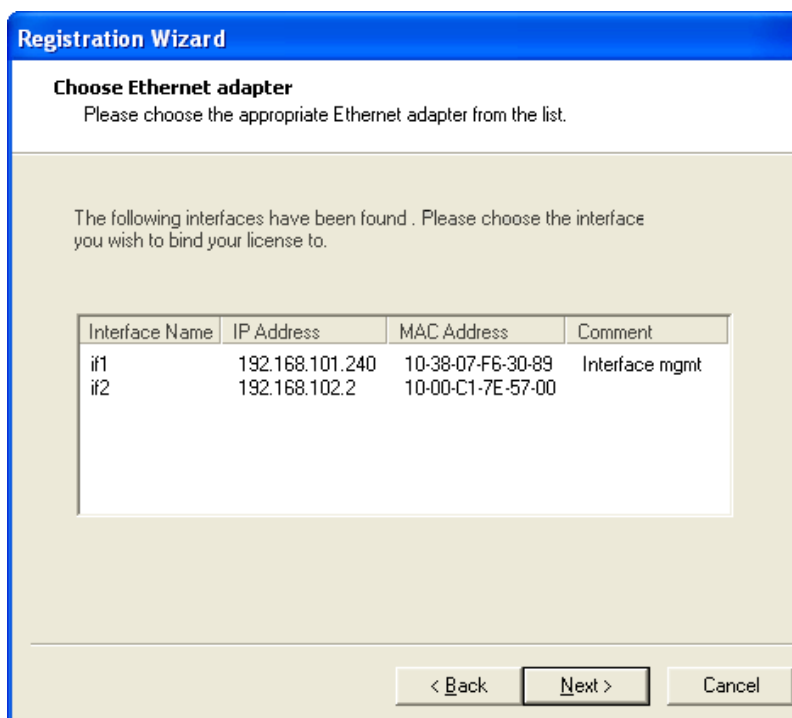
This step is very important, as it creates a unique binding between the Clavister Security Gateway and the license.

2. This page shows all information gathered by the registration wizard. If any data seems to be invalid, the **Back** button can be used in order to go the page containing the invalid data.
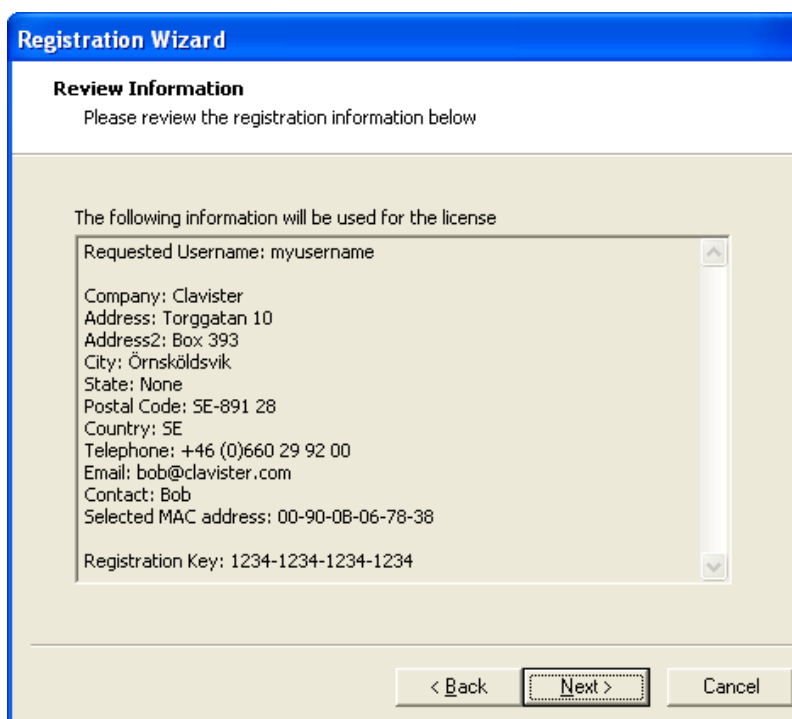
Note

If you are an existing user, this page will not present contact information.

3. All information collected by the registration wizard is now transmitted to the Clavister Client

Web. The Clavister Client Web will generate a unique license, which is then sent back to Fine-Tune.

If, for some reason, any step in the registration process fails, a red "X" mark will be shown in the event list, and a more detailed error message is presented in the status box. A green check-mark will be shown when a step has been carried out successfully.
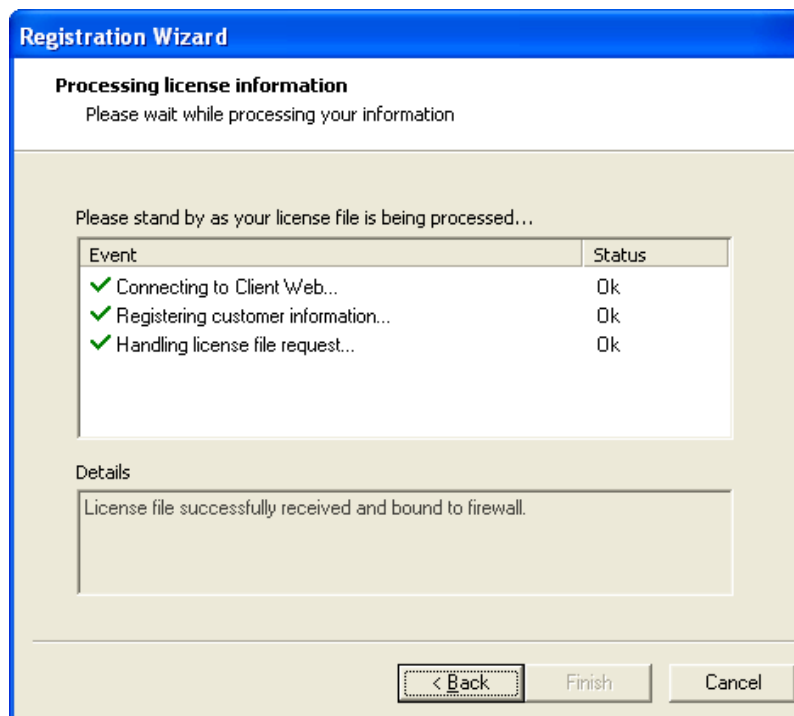
When the license has been successfully received, it will be saved in a sub-directory, named **Licenses**, on the *Management Data Source* that the FineTune resides in. The license can be up-loaded immediately to the Clavister Security Gateway, or at a later time.

The concept of the Management Data Source is explained in the following section

1.4. Management Data Sources

All configuration data used by FineTune is stored as a set of data files. This set of files is referred to as a *Management Data Source*. FineTune is able to use multiple data sources, which is useful if configurations for different Clavister Security Gateways need to be separated for any reason.

Upon installation of FineTune, two data sources are automatically generated; "Default", which is used for standard storage of configurations, and "Samples", which contains a number of pre-defined Clavister Security Gateway configurations that can be used as references.

If the Clavister Security Gateways are to be managed from multiple workstations, the data source should be made accessible to these other workstations by moving it to a file server.

Managing Data Sources

Data sources are managed from the Options dialog box shown below, which can be accessed by choosing **Options** from the **Tools** menu.
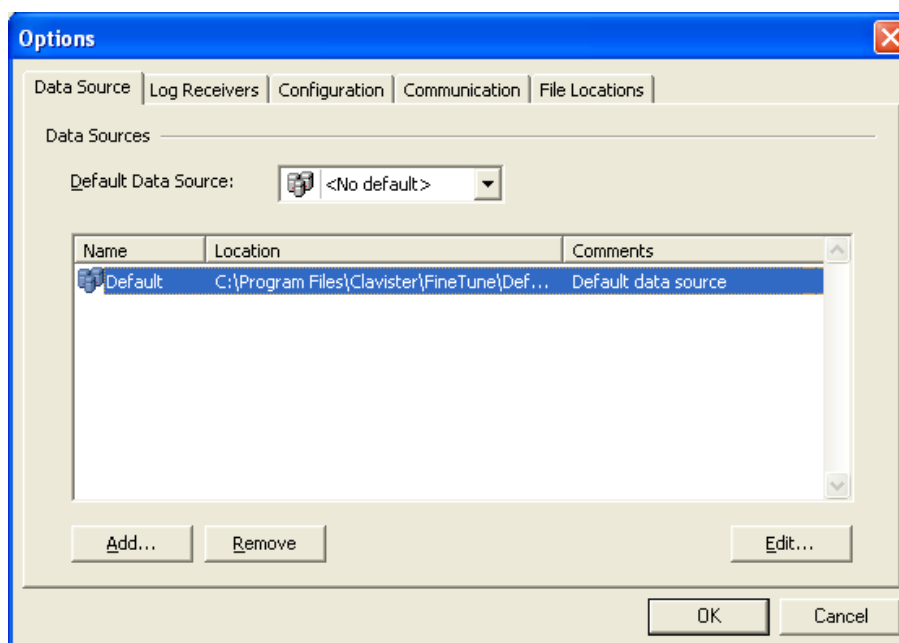
The **Default Data Source** drop-down list specifies the data source that should be used as default in the Security Editor. If none selected, when opening the Security Editor, a selection menu listing all available data sources will be displayed. If you have more then one data source and have specified a default one you can still access the other from the **Tools > Security Editor** menu or by holding the shift key pressed while clicking on the **Security Editor** icon in the left-hand **Tools** toolbar.

Click the **Add** button to add a new data source, or **Remove** to remove a data source. Please note that the actual data files are not deleted when selecting **Remove**

The **Edit** button is used to bring up a dialog where the name and the location of the data source can be modified. Please note that if changing the location of the data source, the actual data files need to be moved manually.

The **Enabled** setting in the dialog box regulates whether the data source should be enabled or not. A disabled data source will not show up in any selection lists.

Data Source Technical Details

The information in this section is provided to give a better understanding of the concept behind data sources. Please note however, that modifying data source files manually is never recommended.

Each data source consists of a set of files that constitutes the definitions and configurations of Clavister Security Gateways, namespaces and folders. There are two main file types, .EFW files and .EFC files. An .EFW file represents a specific gateway, and the corresponding .EFC files contains the different versions of configuration for that gateway.

In the screen shot below, the files in the directory representing the Default data source are listed. For example, the GLOBAL.efw file represents the Global Namespace, and the GLOBAL.00001.efc to GLOBAL.00004.efc contains the four different versions of configuration for Global Namespace.

Name ▲	Size	Type	Date Modified
__efwdb	1 KB	File	2006-08-07 10:47
GLOBAL.00001.efc	7 KB	EFC File	2006-08-07 15:19
GLOBAL.00002.efc	7 KB	EFC File	2006-07-05 14:40
GLOBAL.00003.efc	8 KB	EFC File	2006-08-07 10:49
GLOBAL.00004.efc	8 KB	EFC File	2006-08-07 10:49
GLOBAL.efw	1 KB	EFW File	2006-08-07 14:45
Paris.00001.efc	1 KB	EFC File	2006-08-07 10:46
Paris.00002.efc	12 KB	EFC File	2006-08-07 10:46
Paris.00003.efc	12 KB	EFC File	2006-08-07 10:47
Paris.00004.efc	12 KB	EFC File	2006-08-07 10:49
Paris.00005.efc	12 KB	EFC File	2006-08-07 11:53
Paris.00006.efc	12 KB	EFC File	2006-08-07 15:19
Paris.00007.efc	12 KB	EFC File	2006-08-07 10:47
Paris.efw	1 KB	EFW File	2006-08-07 15:19
Rome.00001.efc	1 KB	EFC File	2006-07-05 14:40
Rome.00002.efc	11 KB	EFC File	2006-08-07 10:49
Rome.00003.efc	13 KB	EFC File	2006-08-07 10:49
Rome.00004.efc	13 KB	EFC File	2006-08-07 14:45
Rome.efw	1 KB	EFW File	2006-08-07 10:46

1.5. Modifying your first security policy

This section provides a quick "walk-through", where the security policy of a newly installed Clavister Security Gateway is being modified. The walk-through assumes that a new Clavister Security Gateway has been installed by following the steps outlined in the Getting Started guide.

In this walk-through, we will use the following example names and IP addresses:

*   The interface chosen as management interface is if1.

*   The IP address of interface **if1** is 192.168.101.240 with netmask 255.255.255.0.

*   The server or workstation running FineTune resides on the same subnet, for instance with an IP address of 192.168.101.100.

*   The Clavister Security Gateway has been given the name **Paris** in FineTune.

> *Note*
> *You will have to substitute the information above with the actual interface name and IP addresses you are using in your specific installation.*

When a new Clavister Security Gateway is first installed and powered-up, the default rule-set of the CorePlus operating system is, as a security precaution, deliberately restrictive:

*   The management server is allowed to remotely manage the Clavister Security Gateway.

*   Hosts residing on networks connected to the **if1** interface are allowed to send ICMP Echo Requests to the Clavister Security Gateway.

*   The Clavister Security Gateway will return ICMP Echo Replies to the requesting host.

All other traffic is unconditionally dropped.

Walk-through

In this walk-through, we will modify the rule-set so that we no longer allow ICMP Echo Requests to be sent to the Clavister Security Gateway. Disabling ICMP Echo Requests may seem unnecessary, but the reason is that this modification to the security policy is easy to understand and to verify with standard tools available on all platforms.

1. We start by verifying that the gateway replies to ICMP Echo Requests. This is performed by using the standard **ping** utility. Open a standard Command Prompt on the management station and leave FineTune running.

    At the command prompt, type:

    ```
    > ping 192.168.101.240
    ```

    Ping should return output similar to the one displayed in the window below. If ping returns a "Request timed out" message, some part of the initial FineTune configuration did not succeed (refer to Appendix A, *Troubleshooting a new gateway*).
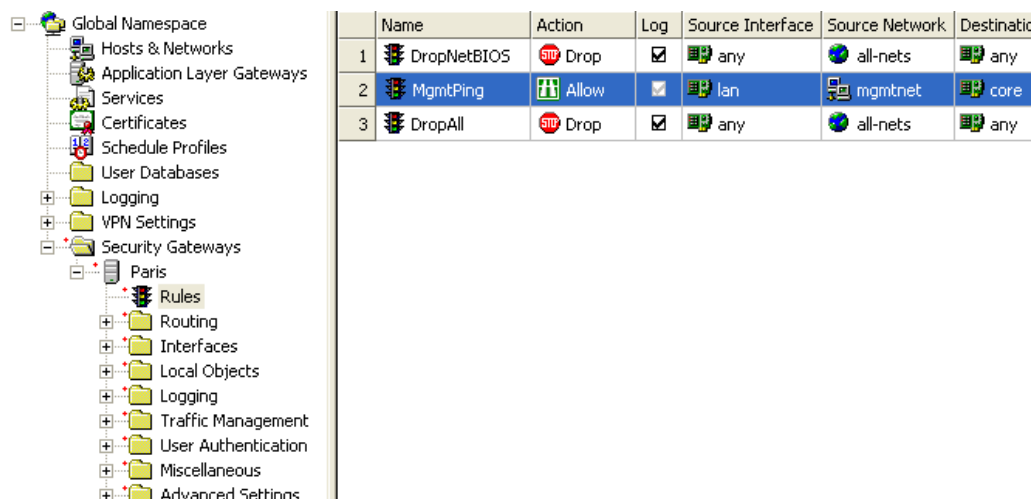
2.   In FineTune locate and select the gateway in FineTune's tree-view. Right-click on the gateway, and choose **Check out** from the **Version Control** submenu. The gateway name and all it's child nodes will appear with small red dots next to the icons to indicate their checked out status.
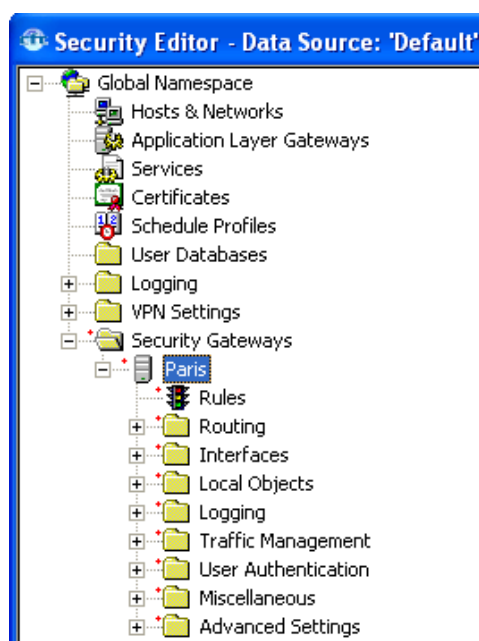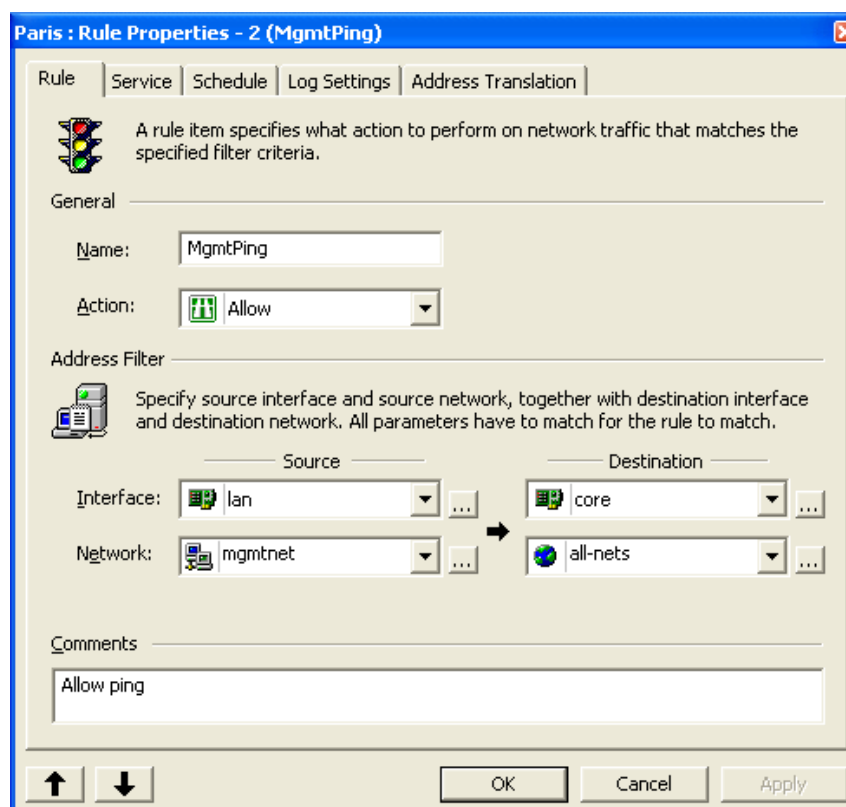
3.   Locate and select the **Rules** node below the gateway node in the tree-view. The rule-set of the gateway will be listed in the grid view as in the screen shot below. Notice the second rule, named *MgmtPing*, in the list. This is the rule that permits ICMP Echo requests.

4. Select the **MgmtPing** rule by clicking anywhere in the row. Right-click and choose **Properties** from the menu shown. The dialog box below will be displayed. Notice the **Address Filter** section, stating that this rule will only match traffic received on **lan** interface and with the **core** interface as destination. (The **core** interface represents CorePlus, and is used when traffic is destined for, and responded to, by the CorePlus itself).

5. Click on the second tab of the dialog box. The **Service** page will be shown. Notice that this rule applies to all ICMP packets.
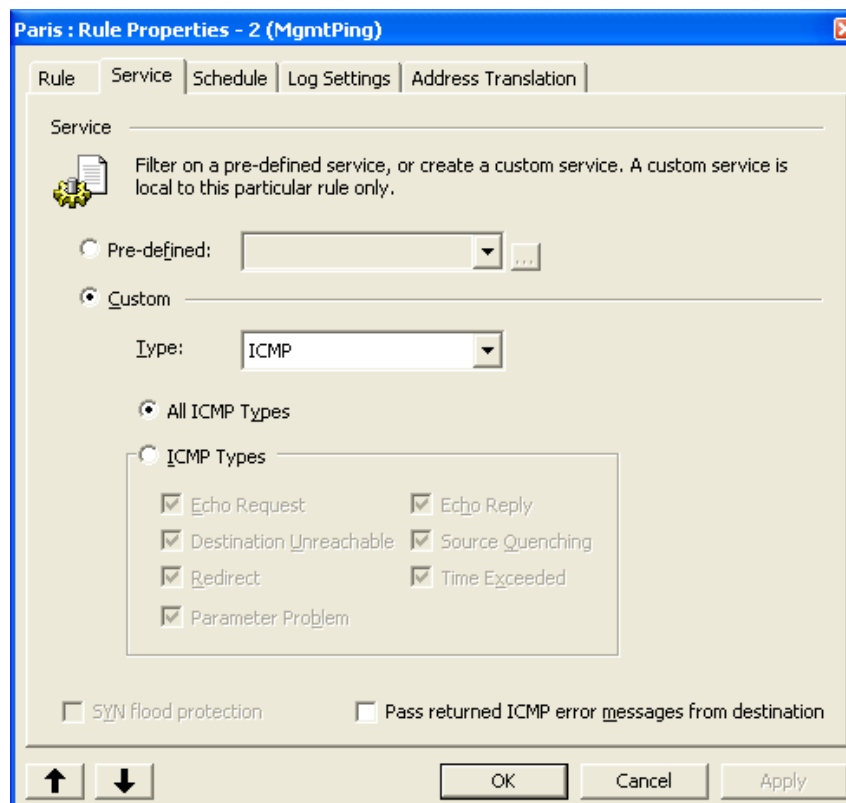
6.   Click on the first tab of the dialog box to switch back to the **Rule** page. Click the arrow button
      in the **Action** drop-down box to display the available actions. Select the action **Drop** This
      changes the rule action to be that of dropping all ICMP Echo Requests to the core, instead of
      allowing them. Close the rule dialog box by clicking the **OK** button.
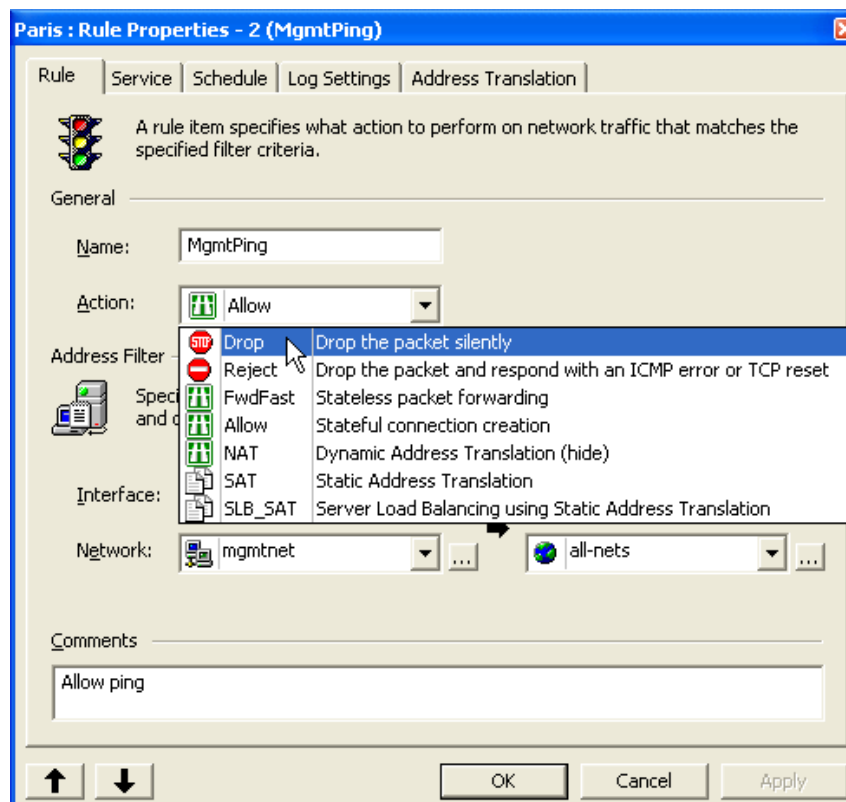
7.   Select the Paris gateway node in the tree view again. Right-click and choose **Check-in** from the
      Version Control submenu. A dialog box similar to the one below will be shown. Enter a com-
      ment for the configuration version you are checking in and click **OK** to close the dialog.
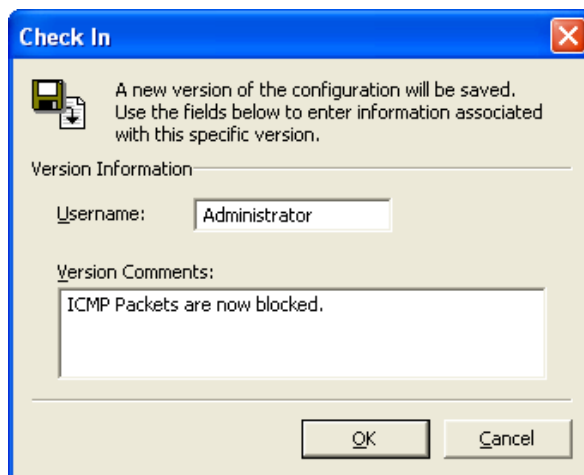
8.   Your Clavister Security Gateway will now be displayed with a blue information icon. Select
      the Security Gateways folder just above your gateway. The list to the right indicates that the
      gateway "Needs deployment". The **DB cfg** column displays *11* while the **Core cfg** column dis-
      plays *6*. This means that the configuration version in the management database is more recent
      than the one running on the gateway.
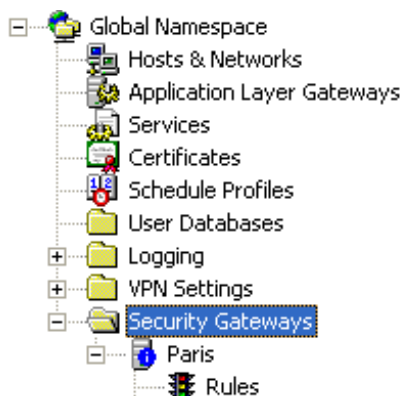
9.   Click the **Deploy Configuration** toolbar button.
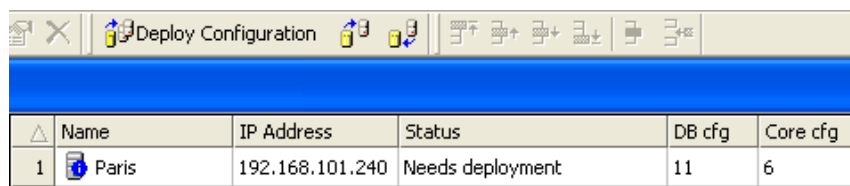
10.   A dialog box similar to the one shown below will be displayed. Click **Next**. The new configur-
      ation will now be uploaded to the Clavister Security Gateway hardware. When the upload is
      finished, the gateway will switch to the new configuration. Click the **Finish** button to close the
      dialog box.
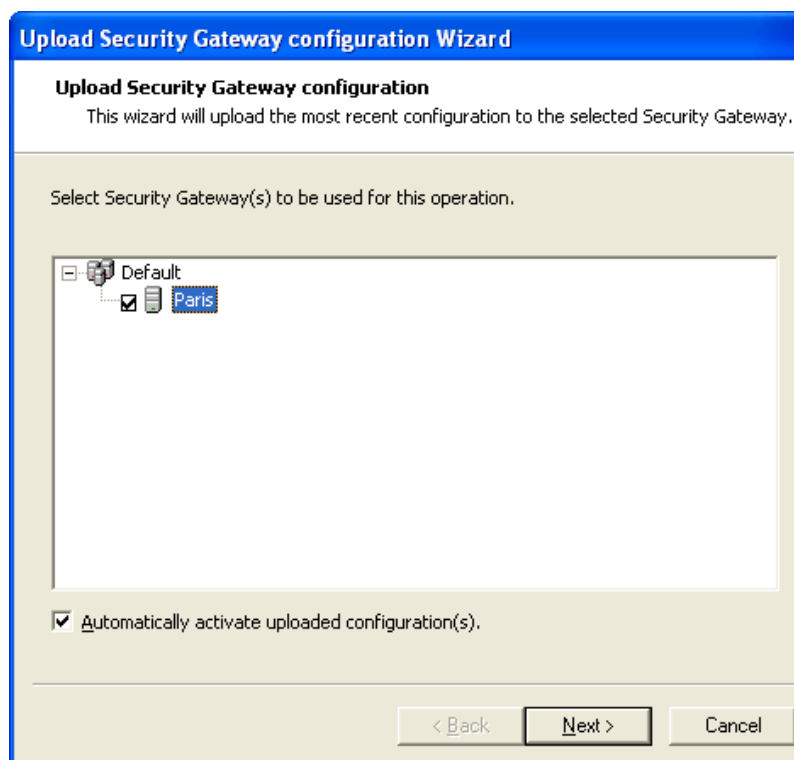
11. The information icon on your Clavister Security Gateway and the "Needs Deployment" status will now disappear. This indicates that the gateway is using the most recent configuration available.

12. Test the new security policy by repeating the ping test. Now the gateway should disallow all ICMP Echo Request packets, and the ping utility will return a "Request timed out" message as shown below.

Congratulations! You have successfully modified your first Clavister Security Gateway security policy.

Note
As the CorePlus rule-set drops all traffic not explicitly allowed, the same result as the above would have been achieved if we had simply removed the entire MgmtPing rule.

However, there are many reasons for why you wish to explicitly drop specific traffic, one example is logging.

Setting up a Log receiver

Now you have set up your first security policy, it's important to remember at this point that no logging will be done from IP traffic or anything else unless you set up a Log receiver. If you haven't done this, refer to Section 5.1, "Clavister Logger" or for a SysLog receiver refer to the CorePlus administration guide.

Chapter 2. Security Editor

The Security Editor is the primary management tool in FineTune. The Security Editor provides an intuitive and user-friendly way of configuring and managing a Clavister Security Gateway. The following major tasks are carried out using the Security Editor:

- Creating, modifying and removing security policies, namespaces and folders

- Clavister Security Gateway and namespace configuration and security policy modifications

- Configuration Version Control

- Clavister Security Gateway communication

- Clavister Security Gateway status monitoring

- Boot media management

- License management

Most of the above tasks are covered in detail by other sections in this documentation. This section will focus only on the actual operation of the Security Editor as a tool.

2.1. Security Editor Layout

The Security Editor tool is launched by clicking on the Security Editor icon which is displayed in FineTune's left-hand toolbar or by choosing **Security Editor** from FineTune's **Tools** menu. If multiple Management Data Sources are activated, a submenu will be displayed allowing the user to choose which data source should be used for this instance of the Security Editor. Please see the section Management Data Sources for more information about how to activate and use multiple management data sources.

A window similar to the one shown below will be displayed.
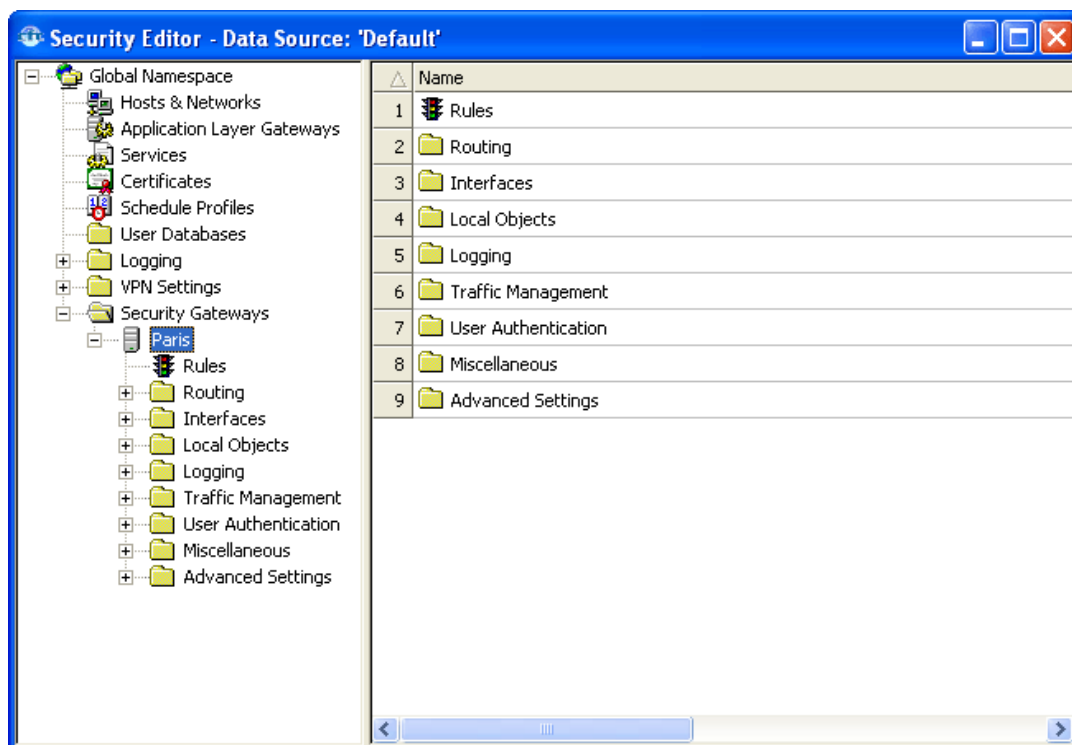
The Security Editor window is divided into two panes. The left pane consists of a tree providing a complete overview of all the nodes in the Management Data Source. This left pane will simply be referred to as "the tree-view". The right pane consists of a grid displaying the contents of the currently selected item in the tree-view. The right pane will be referred to as the grid view throughout this documentation.

Note
You can display the Security Editor in fullscreen mode by pressing F11.

There are several types of nodes that can appear in the Security Editor view. The most common ones are namespaces, folders, Clavister Security Gateways, configuration sections and configuration items.
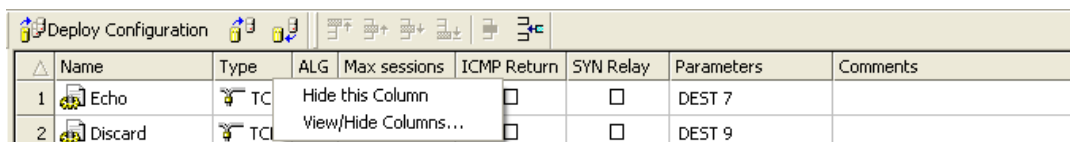
- A *Namespace* is a configurable container that can contain other namespaces, gateways or folders. The **Global Namespace** node in the tree view above is an example of a namespace. For more information about how to use namespaces, please see Section 2.5, "Namespaces".

- A *folder* is similar to a namespace in that it can contain other nodes. A folder is however not configurable. The Clavister Security Gateway node in the tree view above is an example of a folder. For more information about folders, please see Section 2.4, "Folders".

- A *gateway* node represents an installed Clavister Security Gateway. The **Paris** node in the tree view above is an example of this. For more information on how to work with gateway nodes, please see Section 2.6, "Gateways".

- A configuration section resides in a namespace or a gateway. A configuration section represents a subset of a namespace or gateway configuration. The **Services** node in the tree view above is an example of a configuration section. The different configuration sections are explained in detail in the corresponding sections in the documentation.

- A configuration item is the smallest part of a configuration. A configuration item has always a defined type, and configuration items of the same type are collected in the corresponding configuration section. **Http** is an example of a configuration item of the type service, and it therefore resides in the Services configuration section.

28

2.2. Hiding and Un-hiding Grid View Columns

The grid view displays different columns depending on the node currently selected in the tree view.

Some columns may contain information that is rarely used, and for this reason, columns may be displayed or hidden according to the user's needs. To hide a specific column, right-click on the column header of that column. A small pop-up menu as in the screen shot below will be shown. Choose Hide this Column.

To hide or un-hide several columns, choose the **View/Hide Columns** menu option. A window similar to the following will be shown.
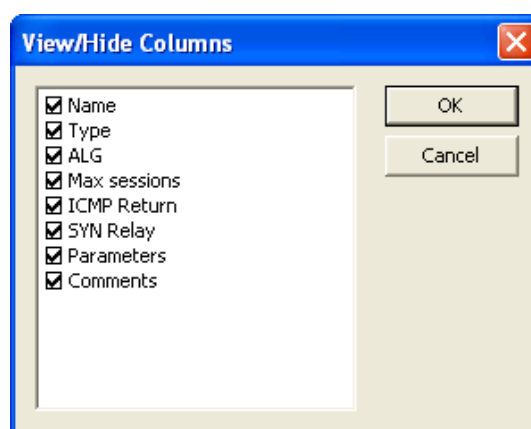
Check or uncheck the columns that should be visible or hidden, and click **OK** to commit the changes.

2.3. Configurations and Version Control

Version control, the ability to save and track changes made to a security policy, is an important tool when managing Clavister Security Gateway configurations. Security administrators need to know what was changed, when it was changed, and who made the changes. To assist administrators with these tasks, FineTunes features a comprehensive version control system, which is an integral part of both the management system and the CorePlus operating system.

Version Control

The version control system in FineTune is designed to track nearly all changes made to a Clavister Security Gateway. Not only IP rule-sets, but entire gateway configurations are subject to strict version control.

This means that whenever a modification to a gateway configuration is done, the actual modification is recorded along with the username of the administrator performing the modification. In addition, the current date and time and an optional version comment is recorded. This scheme allows an administrator to roll back to any given version in time, and deploy that configuration to a running gateway, so that it will operate in the exact same way as it did when the configuration was first created.

The version control system has two key features:

- The ability to archive several configuration versions in the management database.

- The checking out and checking in configurations through the Security Editor.

This section will focus only on how to operate the version control system. For details on how the actual configuration versions are stored, please see Section 1.4, "Management Data Sources".

> ### Note
> *The version control system is enabled from system start and cannot be deactivated. The reason for this is security. All changes to a configuration need to be accounted for. This means that it is important to understand the concept of version control in order to properly manage one or more Clavister Security Gateways.*

Configuration Versions

Each version of a gateway configuration in the management database is associated with a version number, or index, which is set to 1 when the configuration is first created. Every modification of the configuration will generate a new version, with the version number getting incremented by 1. In this way, the most recent configuration version is always associated with the highest version number.

	Name	IP Address	Status	DB cfg	Core cfg	Core ver	Uptime
1	NewYork	192.168.101.241	Down	9	9	8.60.01	-
2	VPN_Demo		OK	5			

The **DB cfg** column of the gateway list in the Security Editor displays the highest version available for each configuration. In normal cases, the highest version in the database is the version being used by the Security Editor for configuration. There are however scenarios when this is not true.

The **Core cfg** column displays the version currently being used by the gateway. If the version number is equal to the **DB cfg** version number, the gateway is using the most recent configuration.

The "Check Out and Check In" Concept

The usage of the version control system is often described as the "Check Out and Check In" concept. The term refers to the operations that an administrator performs in the Security Editor in order to work with gateway configurations. All commands related to version control are accessible

from the **Version Control** submenu available in the **Edit** menu of the Security Editor. The commands are also available as toolbar commands, keyboard shortcuts and from the context sensitive menu brought up by right-clicking an object in the tree-view pane of the Security Editor.

Figure 2.1. The "Check-in" and "Check-out" concept.
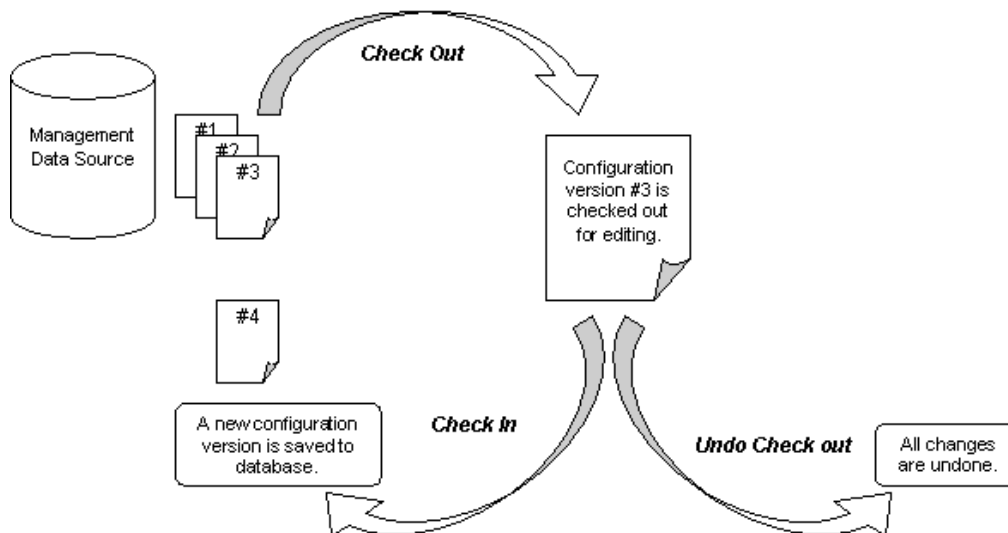
A configuration in the management database can be in one out of two modes, namely "checked in" and "checked out". The default mode is "checked in". An administrator accessing a configuration in "checked in" mode will find the configuration to be read-only, that is, all configuration dialogs are blocked for editing, and no modifications can be done to the configuration. Several administrators may access the same "checked in" configuration simultaneously from different management stations.

Checking out a Configuration

Whenever an administrator wants to start modifying a configuration, the configuration needs to be checked out. This is done by first selecting the actual gateway or namespace that is the target for the modification in the tree-view pane of the Security Editor. Then choose **Check Out** from the **Version Control** submenu, or press **Ctrl+O**.
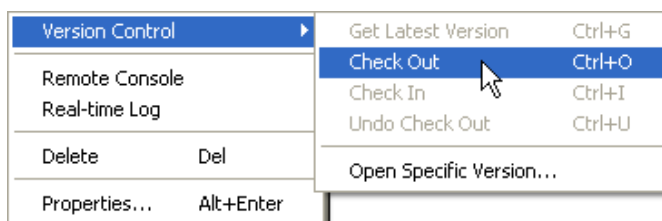
Small red dots in front of the icons in the tree view indicate that the gateway or namespace has been checked out. The administrator who performed the Check Out operation has now exclusive write access to the configuration. As long as the configuration is in "checked out" mode, all attempts to check out the configuration from another management station will fail. This prevents that two administrators accidentally modify the same configuration simultaneously.

Check Out is a recursive operation. This means that if a namespace configuration is being checked out, and the Automatic Configuration Inheritance option is enabled for that namespace, all underlying configurations will be checked out. The reason for this behavior is that a modification of the namespace configuration can affect underlying configurations inheriting the namespace.

The Security Editor will watch for name collisions. When checking out a configuration that contains name collisions, a dialog is shown where these name collisions may be resolved. For more information about name collisions, please see Section 2.7, "Name Collisions".

In a multi-administrator scenario, good practice is that a configuration should not be in "checked out" mode longer than necessary.

Checking in a Configuration

When all necessary changes have been made to the configuration, the administrator needs to perform a check in operation in order to commit the changes to the database. The check in operation stores a new version of the configuration in the management database and changes the mode to "checked in", meaning that the configuration once again is read-only.

To check in a configuration, first select the actual gateway or namespace that should be checked in. Then choose **Check In** from the **Version Control** submenu, or press **Ctrl+I**.

Version Control ▶	Get Latest Version	Ctrl+G
	Check Out	Ctrl+O
Remote Console	Check In	Ctrl+I
Real-time Log	Undo Check Out	Ctrl+U
Delete Del	Open Specific Version…	
Properties… Alt+Enter		

The dialog box shown below will be displayed.

Check In

A new version of the configuration will be saved. Use the fields below to enter information associated with this specific version.

Version Information

Username: Administrator

Version Comments:

OK   Cancel
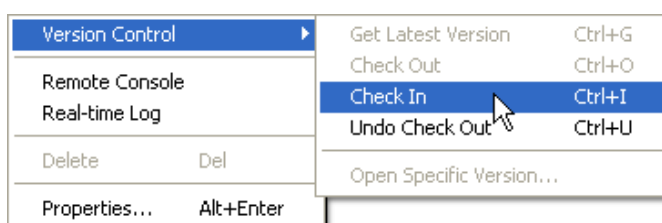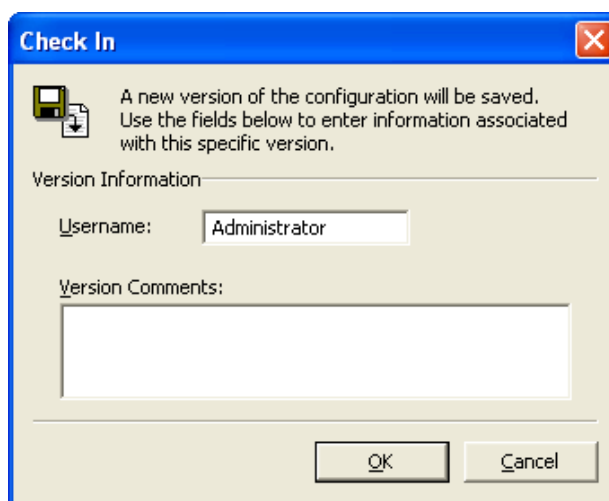
The **Username** field contains by default the Microsoft Windows username of the logged on administrator performing the Check In operation. The **Version Comments** edit box can be used to write a short comment describing the changes made to the configuration. Click **OK** to continue the Check In operation, or **Cancel** to abort and leave the configuration in "checked out" mode.

The **DB cfg** column in the gateway list will now display the new version number. As the **DB cfg** version is now higher than the **Core cfg** version, the Security Editor will notify the administrator that the new configuration needs to be uploaded to the gateway. This is indicated by the text "Needs Deployment" in the **Status** column of the gateway list. Please see Chapter 3, *Remote Management* for more information about communication with the Clavister Security Gateway.

Check In is a recursive operation. This means that if a namespace configuration is being checked in, and any underlying configurations is checked out, the Check In operation will cause all underlying configurations to be checked in as well.

Undoing a Check Out

It is possible to undo all changes made to a configuration. First select the actual gateway or namespace, and then choose **Undo Check Out** from the **Version Control** submenu, or press **Ctrl**+**U** All changes made since the latest check out will be discarded.

Opening a Previous Configuration Version

An administrator can open any of the previously checked in configuration versions. When an earlier version is opened, it will automatically be checked out for editing. If the administrator modifies the opened configuration and checks it in, it will not replace the old configuration. Instead, a new version will be created and thus becomes the latest version in the management database.

To open a previously checked in configuration version, first select the actual gateway or High Availability Cluster, and then choose **Open Specific Version** from the **Version Control** submenu.

The dialog box shown below will be displayed.

This dialog lists all configuration versions checked in since the first creation of the configuration. Apart from the version number, the username, date and time and version comments are displayed for each version. Select the version to open and then click **Open** The selected configuration version will now be read into the Security Editor and automatically checked out.

Get Latest Version

In normal cases, the highest version in the database is the version being used by the Security Editor for configuration. This is however not true when FineTune is used in a multi-administrator scenario.

Consider two administrators, Alice and Bob. They are using the FineTune on different workstations, but connected to the same management database. The database contains, among others, a gateway named Paris. This gateway has undergone a number of configuration changes and has now, say, 42 as its highest configuration version number. The Security Editor in both Alice's and Bob's FineTune correctly reports that the **DB cfg** version is 42.

Now, Alice decides to perform some changes on the Paris gateway. She checks out the gateway, makes the changes and checks it back in. Alice's Security Editor now reports that the DB cfg version is 43 and that a configuration deployment is needed.

Now, what has happened to the Paris configuration in Bob's Security Editor? Actually, nothing has happened. If Bob looks through the configuration of the Paris gateway, he will not be able to detect Alice's changes. This is because he will still be looking at version 42 of the configuration. But, the **DB cfg** column will report that version 43 is the latest version. To make Bob aware that Alice has updated the configuration, the icon of the Paris gateway will be displayed with an Information sign, and the **Status** column will display the text "A more recent configuration version exists in database".

Bob can now choose **Get Latest Version** from the **Version Control** submenu. The latest version available in the database will be read by the Security Editor and replace the current version.
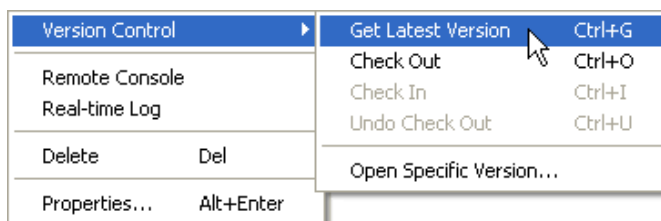
2.4. Folders

A Folder is a simple container that can contain namespaces, Clavister Security Gateways or other folders. Folders in the Security Editor can be compared with the concept of folders in Microsoft Windows explorer.

Folders are especially useful in scenarios where a large number of Clavister Security Gateways are being managed from one single management database. Folders can then be used to group related gateways, for instance according to their geographical location.

Creating a Folder

To create a new folder, locate and select the Clavister Security Gateways node in the namespace where the new folder is to be created. Right-click the selected gateways node and choose **Folder**... in the **New** submenu. A dialog box requesting the name of the new folder is displayed. Enter a descriptive name and click **OK** to create the folder. To abort the creation process, click **Cancel**

Renaming a Folder

To rename a folder, first check out the namespace where the folder resides, then right-click the folder and choose **Properties** from the context menu. A dialog box is shown containing an edit box where the new name can be entered. Click **OK** to save the new name and to close the dialog box. To abort the renaming process, click **Cancel** Finish by checking in the namespace.

Removing a Folder

A folder can only be removed if all underlying nodes first have been removed. To remove an empty folder, right-click the actual folder, choose **Delete** from the context menu and answer **Yes** to the confirmation question.

Note
Removing a folder is an irreversible operation.

2.5. Namespaces

Many of the parameters in a given configuration are common to several, or in some cases, all Clavister Security Gateways within an organization.

Service definitions are good examples of such parameters. The HTTP service, for instance, is most likely to be defined as using the TCP protocol, destination port 80, regardless of which Clavister Security Gateway it is used in. Another example is the **all-nets** network definition, which is defined as network address 0.0.0.0 with a netmask of 0.0.0.0. This definition will be the same for all gateways.

A scenario where a parameter is shared between only some of the gateways might be where three of them are participating in a LAN-to-LAN VPN solution. The Pre-Shared Key and the IPsec proposal lists used by the VPN solution would be common to all three of the Clavister Security Gateways involved. Furthermore, any gateway NOT participating in the VPN solution should not be aware of the Pre-Shared Key in use.

One way of managing shared parameters is to define them individually in each gateway configuration but this can increase dramatically the administrative burden. First of all, the actual operation of creating and managing all parameters will be very time consuming. Secondly, the risk of errors becomes higher as the administrative effort grows. The updating of the Pre-Shared Keys in a large VPN solution soon becomes an administrative nightmare.

FineTune provides a sophisticated solution to this problem by introducing the *Namespace* concept. A Namespace is a container where gateways and folders can be placed. A Namespace can also contain additional Namespaces, meaning that advanced configuration scenarios can be designed. A Namespace can be considered to be a way to group Clavister Security Gateways that have some parameters in common.

In the tree view of the Security Editor, a Namespace is represented as a node with an icon displaying a pair of folders in front of a globe. In the example below, a Namespace called MyNamespace has been created. As can be seen from the example, a number of configuration sections exist in this Namespace. The sections currently available in namespaces are: Hosts & Networks, Application Layer Gateways, Services, Certificates, Schedule Profiles, User Databases, Logging and VPN Settings. The final node is the folder where the gateways (and namespaces) belonging to this Namespace are placed.
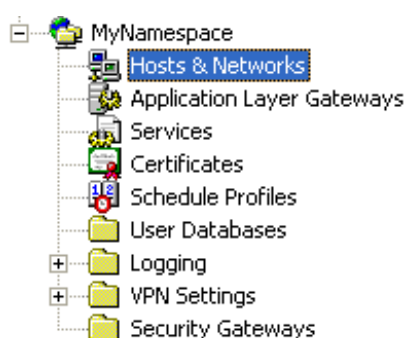
All configuration items defined in a Namespace can automatically be used by all the Clavister Security Gateways (and other Namespaces) defined in that Namespace. This means that if we have defined a network called WebServerNet in a Namespace, we can use this network definition in all the underlying gateways. If we later need to modify that network definition, we only need to modify it in the Namespace; all gateways using the definition will automatically have their configurations updated. (The changes are not deployed to the hardware until the administrator explicitly does the deployment) .

The Namespace concept is most useful when FineTune is used to manage several Clavister Security Gateways, for instance in larger corporate networks or where administration is outsourced to a third-party. But even in smaller installations, with only two or three gateways, Namespaces can significantly simplify day-to-day administration tasks.

The "Global Namespace"

By default, there is always one Namespace created in the Management Data Source. This Namespace is called the Global Namespace and is the root of all gateways and other Namespaces. The Global Namespace is used to define parameters that can be used globally, that is, by all the Clavister Security Gateways in the Management Data Source.

The Global Namespace contains a number of pre-defined configuration items to simplify administration. For instance, the Hosts & Networks section contains the network all-nets, defined as 0.0.0.0 with netmask 0.0.0.0. The **Services** section contains all common service definitions, for instance HTTP, SMTP and NetBIOS. The **VPN Settings** section contains default IKE and IPsec proposal lists.

Naturally, configuration items can be added or modified in the Global Namespace just like in any other Namespace. However, the Global Namespace can neither be deleted nor renamed.

Creating a Namespace

To create a new Namespace, locate and select the Clavister Security Gateways node in the namespace where the new Namespace is to be created. Right-click the selected gateways node and choose **Namespace** in the **New** submenu. A dialog box requesting the name of the new namespace is displayed. Enter a descriptive name and click **OK** to create the Namespace. To abort the creation process, click **Cancel**

Renaming a Namespace

To rename a namespace, first check out the actual namespace, then right-click the Namespace and choose **Properties** from the context menu. A dialog box is shown containing an edit box where the new name can be entered. Click **OK** to save the new name and to close the dialog box. To abort the renaming process, click **Cancel** Finish by checking in the namespace.

Removing a Namespace

A Namespace can only be removed if all underlying nodes in the Security Gateways folder have first been removed. To remove an empty Namespace, right-click the actual namespace, choose **Delete** from the context menu and answer **Yes** to the confirmation question.

Caution
Removing a Namespace is an irreversible operation. The Global Namespace can never be deleted.

A Sample Namespace Scenario

The concept of Namespaces is easier to understand if explained in a context. The screen shot to the right illustrates a sample corporation with four deployed Clavister Security Gateways. Three of the gateways, London, Paris and Rome, are used to interconnect three offices in a VPN. The fourth, Interior, is used to protect an internal network.
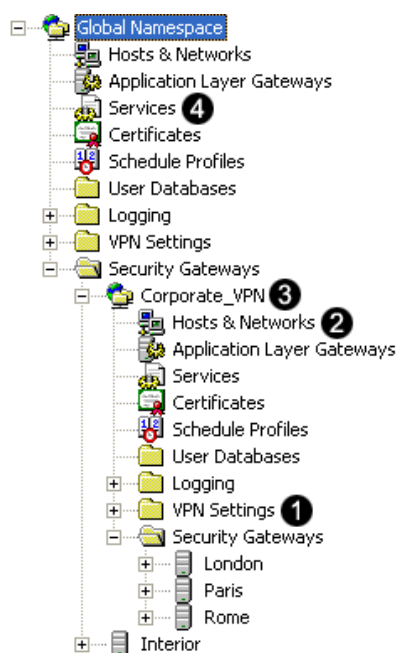
The three VPN gateways share the same VPN parameters, such as Pre-Shared keys and proposal lists. Furthermore, the networks residing behind each gateway need to be known by all three in order for the VPN tunnels to work. For this reason, the administrator of this network has chosen to create a Namespace named **Corporate_VPN** (3). The VPN parameters have been added to the VPN Settings section (1). The network definitions that the VPN gateways need to be aware of have been added to the Hosts & Networks section (2).

The **Interior** gateway is not a member of the VPN, and has thus been placed outside the **Corporate_VPN** Namespace. The result is that the VPN parameters defined under (1) are not available for **Interior** to use.

All of the Clavister Security Gateways, however, use the same set of services for their rule-sets. For instance, HTTP is allowed between the offices (in the VPN), and it is also allowed through the **Interior** gateway. Therefore, all the gateways are using the HTTP service defined in the Services section (4) in the Global Namespace.

Now, the administrator needs to modify the definition of the network residing behind the **Paris** Clavister Security Gateway. This modification is performed in the Hosts & Networks section (2). As all of the VPN gateways use this network definition for their VPN tunnels, the Security Editor will automatically update the three gateways with this new definition. The **Interior** gateway, however, is not affected by the modification.

Automatic Configuration Inheritance

The default mode of operation is that if a configuration item is modified in a Namespace, all underlying gateways using that item will automatically have their configurations updated. This mode of operation is called *Automatic Configuration Inheritance*, and refers to the fact that configuration items are automatically inherited by underlying nodes.

In some scenarios, however, this behavior is not the preferred way of working. First of all, when modifying a namespace, the namespace itself and all the underlying nodes will be locked for editing during the modification operation. In a multi-administrator solution, this can cause unwanted resource conflicts. (This is described in more detail in Section 2.3, "Configurations and Version Control"). Secondly, if different administrators are responsible for the configuration of specific Clavister Security Gateways (eg. in a scenario where Clavister Security Gateway administration is outsourced), an administrator probably prefers to have strict control of all changes made to "their" configurations.

To solve this problem, the Automatic configuration inheritance mode can be disabled for specific namespaces. This is done by un-checking the corresponding checkbox in the properties dialog box

of the Namespace. Please note that the namespace needs to be checked out before any changes can be performed in the properties dialog box.
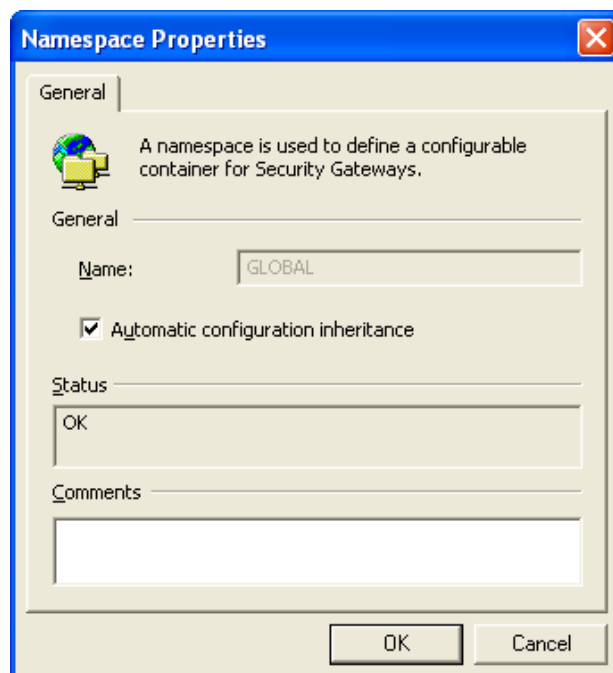
To easier understand how this setting affects the operation, we will use the sample Namespace scenario above. Imagine that we disable Automatic configuration inheritance for the Global Namespace, but leave it enabled for the Corporate_VPN namespace. The behavior of the Corporate_VPN namespace will remain unchanged, which means that a modification to, for example, the VPN Settings section (2) will instantly be reflected by the three VPN gateways.

Modifications to the Global Namespace, on the other hand, will behave differently. First of all, when modifying a Namespace with the Automatic configuration inheritance mode disabled, the operation will no longer lock all underlying nodes. Secondly, underlying gateways will not automatically have their configurations updated.

Instead, when the underlying Clavister Security Gateway gets checked out next time, the administrator will be notified that one or several of the configuration items that the gateway uses have been changed. The administrator can then choose whether to accept the changes or not. This is covered in detail in Section 2.7, "Name Collisions".

2.6. Gateways

Each gateway node in the Security Editor represents an installed Clavister Security Gateway unit. Since they usually represent Clavister hardware installations, these nodes are key nodes in the Security Editor display.

The screen shot below illustrates a sample Clavister Security Gateway node, named Paris as well as it's sub-nodes. The node is illustrated with a server-like icon. Depending on the status of the gateway, the icon can have an overlay image representing an information, warning or error status. For more information about gateway status please see the section called "Monitoring gateway Status".
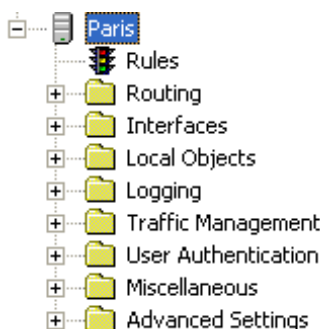
Each Clavister Security Gateway node contains a number of child nodes, mainly folders, each containing the various configuration sections of the device:

Rules	Contains the rule-set, which is the main filtering table of a Clavister Security Gateway.
Routing	Contains all configuration sections needed to configure IP routing in a Clavister Security Gateway. This includes normal static routing as well as Policy-Based routing and DHCP Relay.
Interfaces	Contains interface related configuration sections. For instance, Ethernet adapters, Virtual LANs and VPN tunnels are configured in sections residing in this folder.
Local Objects	Contains configuration sections identical to the ones defined in Namespaces. These include, for instance, Hosts & Networks, Services and VPN Settings. When defining a configuration item in Local Objects, the item will be available to the local Clavister Security Gateway only, as opposed to defining the item in a Namespace, where it will be available to all underlying gateways.
Traffic Management	Contains configuration sections to setup bandwidth management features of the system
User Authentication	Contains user related configuration sections. Add, remove and configure user databases and rules for user authentication.
Miscellaneous	Contains the configuration sections Access, Remotes and Pipes. The Access section provides anti-spoofing capabilities. The Remotes section configures remote management and the Pipes section is used for Traffic Shaping functionality.
Advanced Settings	Contains parameter settings for operation of the Clavister Security Gateway. These include protocol time-outs, header lengths, IP options, TCP flags etc.

All the configuration sections together build up the entire configuration which is used at run-time.

Clavister Security Gateway Types

The Security Editor defines three types of Clavister Security Gateways:

Appliance   Represents a Clavister Security Gateway from the Clavister hardware series of products. When installing an appliance, major parts of the configuration, for instance, interfaces, routing and so forth, are auto-generated.

Software   Represents a Clavister Security Gateway based on non-Clavister hardware. This involves installed the CorePlus operating system on non-Clavister hardware. Installation and management are similar to an appliance, but involve creating boot medias. (Boot medias are not required with Clavister hardware).

Custom   A custom Clavister Security Gateway is used when no auto-generation of configuration is needed. A custom type is a gateway node with an, initially, empty configuration. This type is recommended for use by experienced users only.

There is also one additional pseudo-type of Clavister Security Gateway the High Availability cluster, which is actually several Clavister Security Gateways working as one. For more information about High Availability clusters and please refer to the CorePlus Administration Guide.

The type of the Clavister Security Gateway is only important in the creation process. In operation, all gateway nodes look and behave the same in the security editor. The only restriction is for nodes of the *Appliance* type, (ie. Clavister hardware based) on which boot media operations are not permitted.

Creating a Gateway

To create a new gateway, locate and select the gateway's node in the Namespace where the new gateway is to be created. Right-click the selected gateway's node and choose **Gateway** in the **New** submenu. The New Security Gateway Wizard dialog box will be displayed.

Modifying Gateway Properties

A gateway node contains, except for the gateway run-time configuration, a number of properties used to describe the gateway. For instance the name of the gateway and how FineTune should communicate with it.

To modify the properties of a Clavister Security Gateway, first check out the gateway, then right-click it's node and choose **Properties...** from the context menu. A dialog box similar to the one below is shown.
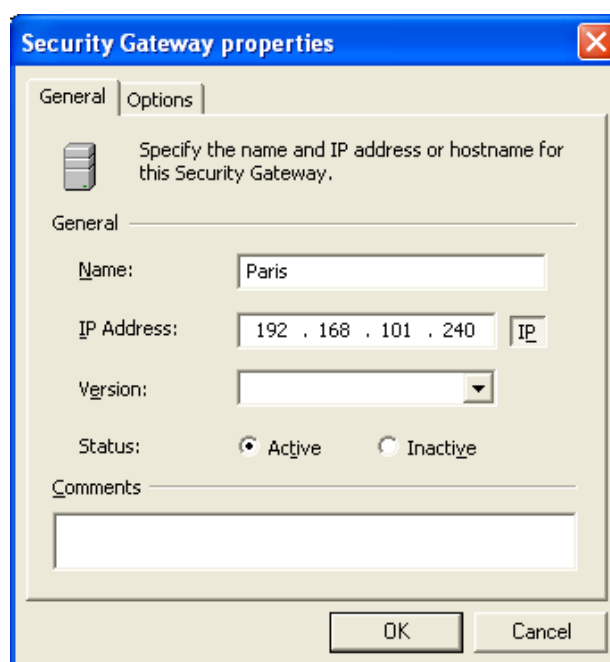
Name   The name of the Clavister Security Gateway. Most tools in FineTune use the gate-
                  way name to identify the specific device. As the name is also used in log analyz-
                  ing, it is not recommended to change the name of a running gateway unless abso-
                  lutely necessary.

IP Address   This is the IP address of the gateway. Normally, this is the IP address of the inter-
                  face that was chosen as management interface during the installation. FineTune
                  uses this IP address for remote communication purposes. However, this setting
                  will not affect how the gateway will be configured.

                  De-selecting the **IP** button will change the **IP Address** field to a hostname field.
                  FineTune supports using standard DNS resolving to get the IP address of the gate-
                  way. This option is only recommended if the IP address of the gateway is dynam-
                  ic, for instance if DHCP client support is activated in the gateway.

Version   This is the version of the CorePlus software in use.

Status   The status of the gateway. FineTune will not perform status monitoring of gate-
                  ways marked as *Inactive*.

Comments   Optional comments, for instance gateway location, product model etc.
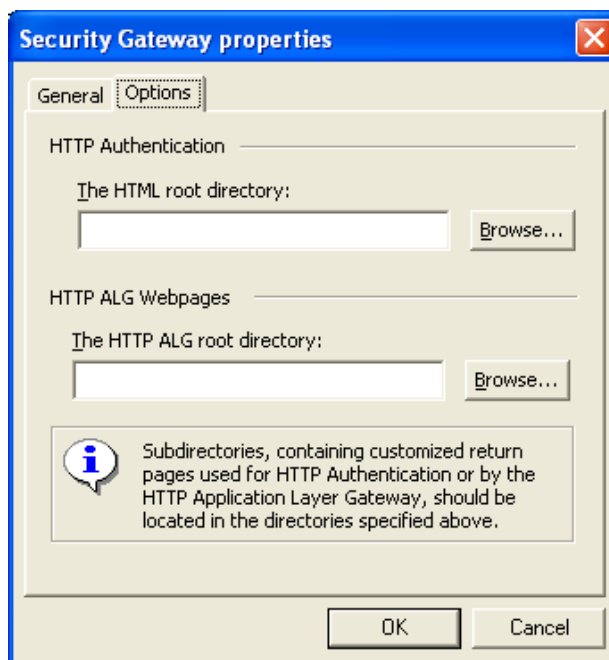
The HTML root directory   This is where the customized HTML pages are stored, related
                                        to user authentication.

The HTTP ALG root directory   This is where the customized HTML pages are stored, related
                                        to the HTTP ALG. These are presented to the user if this
                                        ALG blocks content.

Click **OK** to save the properties and to close the dialog box. Finish by checking in the gateway.

> *Note*
> *Changing settings in the properties dialog box will not make any changes to the gate-*
> *way itself. Changing the IP Address in this dialog box, for example, will only change*
> *the IP address stored in the management database and used for management commu-*
> *nication with the gateway.*

Removing a gateway

To remove a gateway, right-click the actual gateway, choose **Delete** from the context menu and an-
swer **Yes** to the confirmation question.

> *Note*
> *Removing a gateway is an irreversible operation.*

Monitoring gateway Status

Each gateway has a status, representing it's health. The status is used to indicate, for instance, con-
figuration related errors or runtime problems. The icons of the gateways in the tree view of the Se-
curity Editor will change shape according to their status, and the Status column in the gateway list,
shown below, will present the status in clear-text.

△	Name	IP Address	Status	DB cfg	Core cfg	Core ver	Uptime	Last Modified	Subscription valid until
1	Paris	192.168.101.240	OK	13	13	8.60.01	4 hours	2006-08-03 10:41	2008-08-25

An example of a status is Configuration error, which indicates that the corresponding gateway has a
severe problem with its configuration. Not all statuses are severe. For instance, the status *Needs de-*

ployment is not a critical status at all. For this reason, each status is assigned a status level. There are four status levels: *Error, Warning, Information, Ok* in order of importance.

A gateway can have several simultaneous statuses, but only the status with the most important status level will be shown. A status indicating that the gateway is unreachable, for instance, will have precedence over the Needs deployment status.

FineTune uses the NetCon remote management protocol to periodically query active Clavister Security Gateways for information. In this way, FineTune is able to detect if a gateway is reachable or not. Furthermore, the information returned from the gateway contains important information such as the version of the running configuration, the gateway CorePlus version and capabilities, gateway uptime etc.

The table below lists all possible statuses, their meaning and what actions that are proposed in order to solve the potential problem.

Table 2.1. Gateway Status

	Status level	Status	Meaning	Proposed Actions
	Ok	Ok	The gateway is up and running.	None
	Information	Demo mode	The gateway is running in demo mode.	If a license has been purchased, register the gateway by selecting the gateway and choosing **Register** from the **Action > License** menu.
	Information	Needs deployment	The Management Data Source has a more recent version of the gateway configuration.	Click the **Deploy Configuration** toolbar button. See Section 3.3.2, "Deploying a configuration" for more information.
	Information	Needs deployment	The Management Data Source has a more recent version of the gateway configuration.	Click the **Deploy Configuration** toolbar button. See Section 3.3.2, "Deploying a configuration" for more information.
	Information	Empty configuration	The configuration is empty.	For custom type gateways, check out the gateway and add configuration items manually. For HA Clusters, add cluster members to the cluster by right-clicking the Cluster Members folder and choosing **High Availability Master** from the **New** submenu.
	Information	A more recent configuration exists in data source	The configuration has been modified from another FineTune installation, or by using the text-mode editor.	Right-click the gateway and choose **Get Latest Version** from the **Version Control** submenu.

	Information	Needs configuration download	The gateway has a more recent version of the gateway configuration.	Select the gateway and download the latest configuration. See Section 3.3.3, "Downloading a configuration" for more information.
	Information	The Software Subscription will expire in less then two weeks	After the software subscription period has expired, it is not possible to upgrade CorePlus to a new version.	If you are planing to upgrade the gateway after this two week period you need to download an updated version of the license from the ClientWeb and if necessary buy a subscription.
	Warning	License file on gateway, missing in data source	The gateway has a valid license, but the license file is missing in the data source.	Download the license from Clavister Client web.
	Warning	Configuration warning(s)	The gateway configuration contains one or more warnings.	Right-click the gateway and choose **View Warnings and Errors** in the context menu to see the configuration warnings.
	Warning	One or more child nodes are down	One or several gateways in this namespace has been reported as down.	Expand the gateways folder in the namespace to locate the faulty gateways.
	Warning	One or both cluster members are down	One or both cluster members in this HA Cluster has been reported as down.	Expand the Cluster Members folder in the namespace to locate the faulty gateways.
	Warning	License bound, but missing on gateway	The gateway has been registered and a license has been retrieved from Clavister Client web, but the license has not been uploaded to the gateway.	Select the gateway and choose **Upload License** from the **Action > License** menu.
	Warning	Uses default management keys	The gateway is using default management keys, which is a security problem.	Select the gateway and choose **Change Remote Management Keys** from **Action > Communication** menu.
	Error	Text-mode only	The Security Editor was unable to parse the configuration. Only the text-mode editor can be used to modify the configuration.	Open the text-mode editor by selecting the gateway and choosing **Edit Configuration in Text-mode** from the **Edit** menu.
	Error	Incomplete configuration	The New Clavister Security Gateway wizard was aborted before the gateway configuration was downloaded.	Right-click the gateway and select **Resume New Security Gateway wizard** from the context menu.

	Error	Error parsing the configuration file	The Security Editor was unable to parse the configuration due to severe errors in the configuration.	Right-click the gateway and choose **View Warnings and Errors** in the context menu to see the configuration errors.
	Error	Down	Clavister FineTune is unable to contact the gateway.	Read Appendix A, *Troubleshooting a new gateway*. Revert to Default Remote Management Keys.
	Error	Lockdown: By the 'lockdown' console command	The command 'lockdown on' has been issued on the gateway console. Only traffic from management networks to the gateway itself is allowed.	Issue the command 'lockdown off' on the gateway console.
	Error	Lockdown: License problem	The license file on the gateway is invalid. This will occur if the license file has been manually modified, or if the gateway hardware has been replaced (MAC address mismatch). Only traffic from management networks to the gateway itself is allowed.	If the license file on the gateway has been modified, upload a valid license by selecting the gateway and choosing **Upload License** from the **Action > License** menu.
	Error	Lockdown: Configuration problem	The gateway configuration is invalid. Only traffic from management networks to the gateway itself is allowed.	Contact your reseller or system integrator for technical support.
	Error	Lockdown: Reason unknown	The gateway has been locked down for an unknown reason. Only traffic from management networks to the gateway itself is allowed.	Contact your reseller or system integrator for technical support.
	Error	Not a valid entry	The entry for this gateway in the Management Data Source is invalid. The data base is most likely corrupt.	Contact your reseller or system integrator for technical support.
	Error	Not a valid configuration	The configuration data for this gateway in the Management Data Source is invalid. The data base is most likely corrupt.	Contact your reseller or system integrator for technical support.

2.7. Name Collisions

When a gateway (or namespace) is being checked out, the Security Editor checks for Name collisions. This is done by comparing all configuration items in the configuration being checked out, with the corresponding items in the namespaces that the gateway (or namespace) resides in.

If the Security Editor encounters two configuration items with the same name, but with different definitions, it is considered a name collision, and a dialog box similar to the one shown below is displayed.

Name collisions can be caused by a lot of reasons. One could be the scenario discussed in the previous section; the administrator modifies a configuration item in a namespace with the Automatic configuration inheritance option disabled. The result will be that the namespace has a new definition of the actual configuration item, while the underlying gateways have their old definitions of the same item. When the administrator later checks out one of the underlying gateways, the name collision is detected.

The Name Collisions Dialog Box

When one or more name collisions have been detected, the Security Editor displays the Name Collision dialog box shown below.
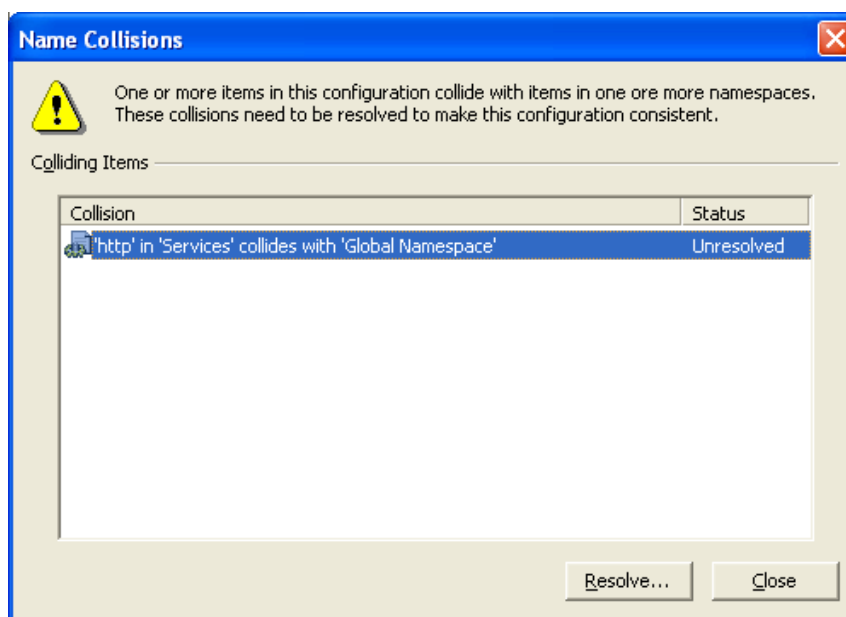
The dialog box contains a list of all the items that are causing collisions. The first column in the list gives a short explanation about the collision, and the second column displays the resolving status. The status is set to **Unresolved** by default.

Clicking the **Resolve** button will allow the administrator to resolve the collision. See the section called "Resolving Name Collisions".

Clicking the **Close** button will close the Name Collisions dialog box and continue the check out process.

> *Note*
> *It is possible to leave collisions in an unresolved state and close the Name Collision dialog box. However, the next time the actual gateway gets checked out, the unresolved items will cause the Name Collision dialog box to be displayed again.*

Resolving Name Collisions

In the sample Name Collision dialog box above, one collision has been detected when checking out the *Paris* gateway. In this case, it is the http service definition that collides with the http service defined in the Global Namespace.

To resolve the collision, click the **Resolve** button. A Resolve dialog box similar to this one is displayed.
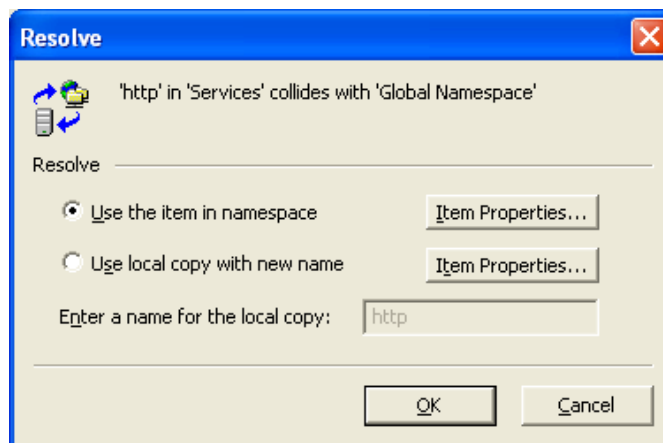
There are two possibilities to solve the name collision:

Use the item in namespace	Selecting this option will cause the local definition of the item to be discarded and replaced by the definition in the namespace.
Use local copy with new name	Selecting this option will cause the local definition of the item to be saved. Note that a new name has to be given the item; otherwise it will continue causing a collision.

To find out the differences between the two colliding definitions, the **Item Properties** buttons can be used. The top button will display the item properties as defined by the namespace. The bottom button will display the item properties as defined by the local gateway. Both dialog boxes can be displayed at the same time in order to simplify item comparison.

Consider an example where the two dialog boxes are displayed. The Global Namespace dialog shows the http service definition. The other dialog box displays the properties for the http service definition in the *Paris* gateway. The difference between the two definitions might be that the destination port number has been changed to 81 in the Global Namespace, while it is still defined as port 80 in the *Paris* gateway.

If this is the case, the administrator can choose the **Use the item in namespace** option, then the http definition in the Interior gateway will be copied from the Global Namespace, and will therefore start to use port 81. If instead the administrator chooses the **Use local copy with new name** option, and enters a new name, for instance, local_http, then the local_http service will keep its destination port 81. All references to http in the *Paris* configuration will be replaced with local_http.

2.8. Working with Configuration Items

A configuration item is the smallest part of a configuration. A configuration item has always a defined type, and configuration items of the same type are collected in the corresponding configuration section. Each configuration item has a definition, which describes the actual configuration item. The table below lists some sample configuration items, their definitions and their corresponding configuration section.

Table 2.2. Sample Configuration Items

Configuration Item	Definition	Configuration section
http	Protocol: **TCP**, Destination port: **80**	Services
smtp	Protocol: **TCP**, Destination port: **25**	Services
all-nets	Network: **0.0.0.0**, netmask: **0.0.0.0**	Hosts & Networks
gw-world	Host: **192.168.0.1**	Hosts & Networks
vlan1	Interface: **if1**, VLAN: **ID1**	Virtual LAN
DropAll	Action: **Drop** Source Interface: **Any** Source Network: **all-nets** Destination Interface: **Any** Destination Network: **all-nets** Serice: **Any**	Rules

Each configuration item type has a specific purpose in a gateway configuration. A Services configuration item, for instance, is a definition of a specific protocol. An Ethernet configuration item describes a physical Ethernet interface in the gateway. Rule configuration items build up the IP rule-set.

This section gives an overview of how to work with configuration items, that is, with operations that are common to all items. It does not explain how the different configuration items work, or how they will affect a gateway configuration. This information is available in the various sections that describe the different CorePlus features.

Configuration items are listed in a table format in the grid view of the Security Editor. The configuration items belonging to a specific configuration section are displayed when that section is selected in the tree view. In the screen shot below, the Services configuration section has been selected in the tree view, and the Services configuration items are listed in the grid view.

Adding a Configuration Item

To add a configuration item, first select the appropriate configuration section, then right-click and choose **New <Item>**... from the context menu (<Item> being the actual configuration item that is being added). An item can also be added by right-clicking in the grid view and choosing **New <Item>** from the context menu. If no item is selected, the new item will be added at the bottom of the section, otherwise it will be added above the selected item.

A properties dialog box corresponding to the type of the item added will be displayed. Fill out the dialog box and click the **OK** button to save the new item or click **Cancel** to abort.

> ### Note
> *The configuration needs to be checked out for the above operation to work.*

Removing a Configuration Item

To remove a configuration item, select the actual item, right-click the item, choose **Delete** from the context menu and answer **Yes** to the configuration question. If the configuration item is in use by other configuration items (for instance, a Rule using a network definition), the delete operation will fail. To remove a configuration item that is in use, all the referring items has be either removed or modified first.

> ### Note
> *The configuration needs to be checked out for this operation to work.*

Modifying a Configuration Item

To modify a configuration item, select the actual item, right-click the item and choose **Properties** from the context menu. The properties dialog box for the actual item type is displayed. Modify the parameters as needed, and click **Ok** to save the changes or **Cancel** to undo the modifications.

> ### Note
> *The configuration needs to be checked out for this operation to work.*

In-Cell Editing

As a complement to using dialog boxes for working with configuration items, an administrator can choose to enable In-Cell Editing. When In-Cell Editing is activated, modifications to a configuration item can be performed directly in the grid view. Please note, however, that not all configuration item parameters are accessible from the grid view.

In-Cell Editing mode is disabled by default but may be activated by checking the Enable In-Cell editing check box in the **Configuration** page of the **Options** dialog box. The **Options** dialog box is displayed by choosing **Options** in the **Tools** menu.

Moving Configuration Items within the Same Section

Configuration items can be moved within the same section. This is particularly useful in configuration sections where the order of items is important, for instance in the Rules section, but also for other sections, moving items might be necessary.

To move a configuration item, first select the item in the grid, then right-click the item and choose the appropriate move command from the **Row** submenu. The **Row** toolbar, shown below, can also be used to perform move operations.

Figure 2.2. The Row Toolbar
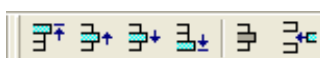
Note

The configuration needs to be checked out for this operation to work.

Comment Rows

Comment rows are useful to add informative comments to a configuration section, or to "group" items to have a better overview.

A comment row is added by first selecting an item, and then right-click the item and choose **Insert comment Row** from the **Row** submenu. A dialog box querying for the comment text is displayed. Enter the comment and click **OK** to insert the comment. The **Row** toolbar can also be used to insert comment rows.

60	knetd	TCP			☐	☐	DEST 2053
61	man	TCP			☐	☐	DEST 9535
62	UDP based services						
63	rlp	UDP			☐	☐	DEST 39
64	bootps	UDP			☐	☐	DEST 67

In the screenshot above, a comment row stating "UDP based services" has been inserted into the Services section to divide TCP and UDP based services.

Note

The configuration needs to be checked out for this operation to work.

Disabling Rows

In some occasions, for instance, when testing how specific rules affect the network traffic, it might be useful to disable a configuration item instead of removing it.

To disable an item, first select the item in question, and then right-click the item and choose **Disable Row** in the **Row** submenu. Enable the item by repeating the operation. The disable command is also available from the **Row** toolbar.

In the screenshot above, the rule DropNetBIOS at row 1 has been disabled and will therefore not be used by the gateway.

Note

The configuration needs to be checked out for this operation to work.

Moving Configuration Items to a Namespace

As explained in the Namespaces section, in some scenarios, there are administrative benefits of having configuration items, for instance Hosts & Networks definitions, shared between several gateways. When installing a new gateway, definitions are stored in the Local Objects section of the new gateway. The exception is if a duplicate of a definition was found in a namespace, then the namespace definition will be used, and the local definition will be discarded.

Imagine a scenario where two gateways, named Paris and London, are going to participate in a LAN-to-LAN VPN. Each gateway needs then to be aware of the other gateway's "remote network", that is, the protected networks that the VPN tunnels give access to. The network protected by Paris is named **if2net**, and so is the network protected by London. The networks are defined in the Local Objects sections when the gateways are first installed, meaning that one gateway is not aware of the other's network definitions.

Instead of creating duplicates, a better solution would be to move the network definitions to a namespace, so both gateways can start using each other's definitions. First select the configuration items that are to be moved, and then right-click and choose the **Move to Namespace** in the context menu. A dialog box similar to the one shown below is displayed.
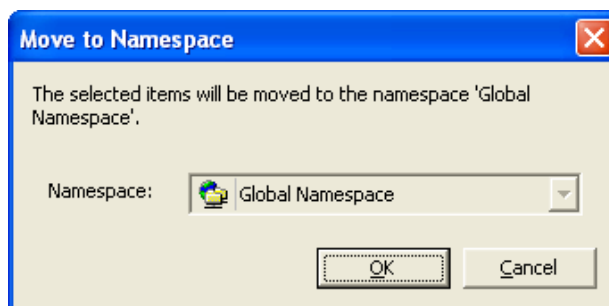
The target namespace can be selected in the dropdown combo-box. If there are no other namespaces than the Global Namespace, then no selection is permitted. Click **OK** to confirm the move, or **Cancel** to abort the operation.

To avoid duplicate names, the gateway name is added as a prefix to the item name. In the sample scenario above, moving the two **if2net** definitions would have resulted in the networks **Paris_if2net** and **London_if2net**.

The process of moving configuration items to a namespace is an irreversible operation. The only method of moving items back is to manually create new items and to update all references to the items.

Note

Both the target namespace and the source gateway need to be checked out for this operation to work.

Configuration Item Usage

As previously mentioned, the Security Editor keeps track on what configuration items are used by what gateways and in which configuration sections.

To find out where a specific configuration item is used, the Security Editor provides a **Usage** property page where this information is presented. The **Usage** property page can be found in all dialog boxes containing **Properties** for configuration items that can be used by other configuration items.

In the sample dialog box below, the **Usage** property page for the all-nets configuration item is shown. The list in the property page reveals that **all-nets** is currently being used by various sections of the Paris gateway. The first column of the list displays the name of the gateway and the name of the configuration section. The second column displays the row number of the item, and the last column displays the name of the item, if any.
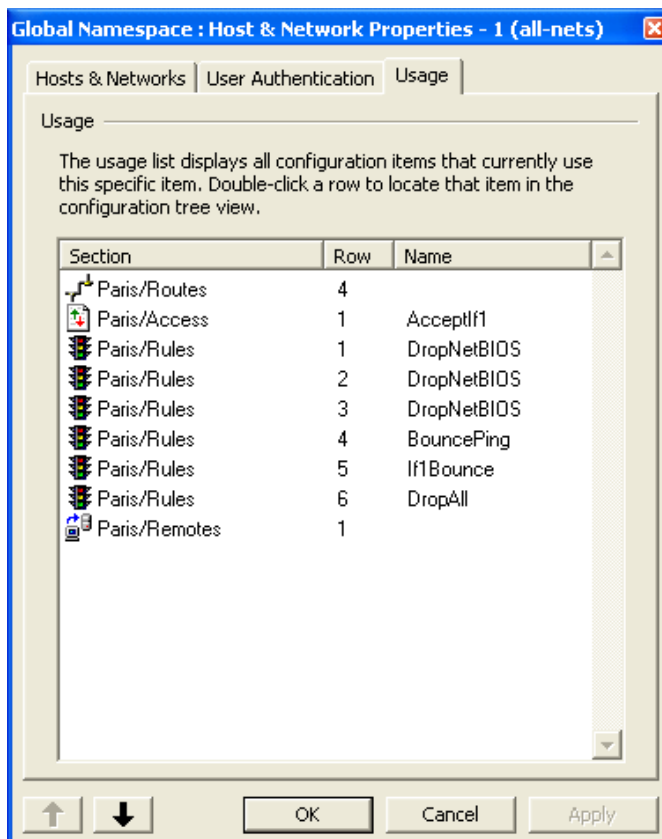
Any of the configuration items in the list can be located in the Security Editor simply by double-clicking on the item. The corresponding gateway and section will be selected in the Security Editor, and the item will be highlighted in the grid view.

Note
The usage list is invalid for items belonging to a namespace with the Automatic configuration inheritance option disabled.

2.9. Working with Groups

Some types of configuration items may be grouped to simplify the security gateway configuration. Hosts & Networks, Services and Interfaces are examples of items that can be grouped.

Adding Configuration Items to Groups

The procedures involved with managing groups are similar, independent of group type. In these examples, an Interface group will be used to demonstrate the operations.

In the sample below, an interface group has been created with no interfaces added so far. To add one or more interfaces to the group, click the button illustrated with a green plus sign. A selection dialog box similar to the one shown below will be displayed.
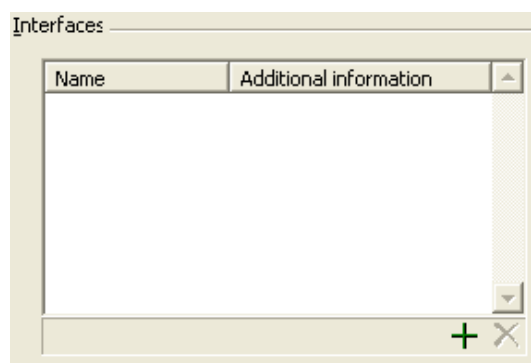
Select the interfaces from the list that should be added to the group. To select multiple interfaces, press and hold the Ctrl or Shift key while clicking the interfaces.
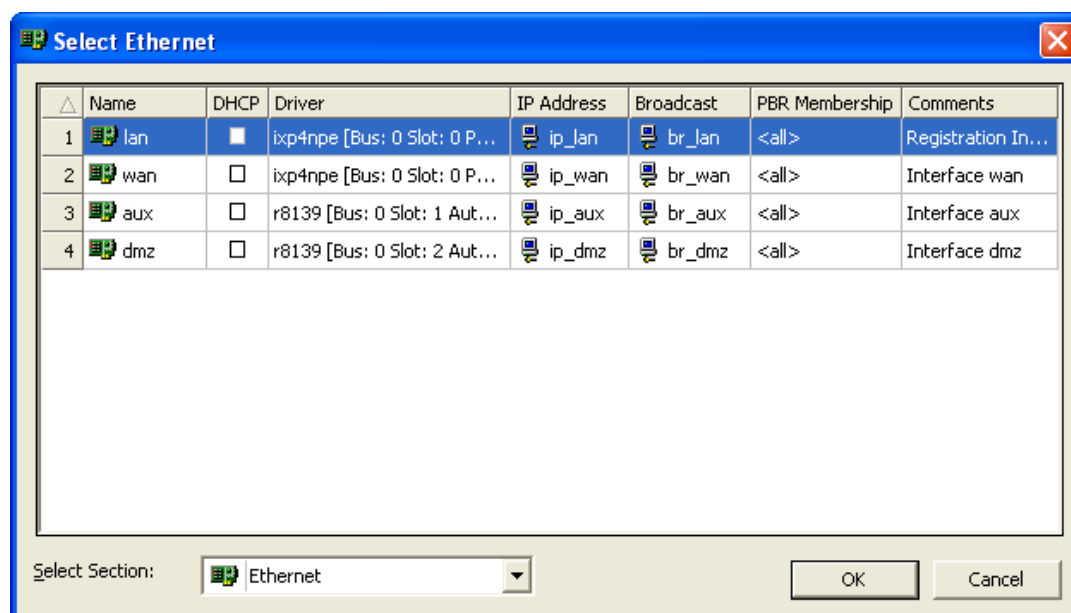
Some groups can contain different types of items. An interface group, for instance, can contain Ethernet interfaces, Virtual LAN interfaces and VPN Tunnels. In these cases, the **Select Section** drop-down list is displayed in the selection dialog box. Choose a section from the drop-down list to display the configuration items from that section.

Click **OK** to close the selection dialog box and add the selected items to the group.

Removing Configuration Items from a Group

To remove configuration items from a group, first select the items to be removed in the group list.
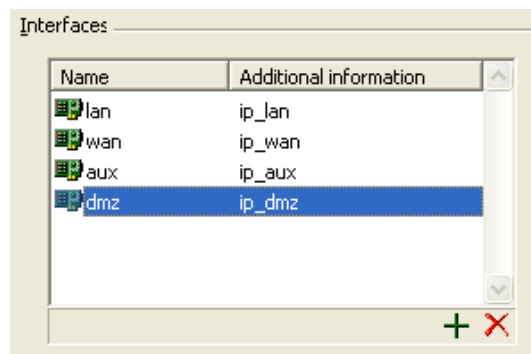
Press and hold the Ctrl or Shift while selecting to include multiple items in the selection. Click the button illustrated with a red X. The selected items will now be removed from the group.

2.10. Text-mode Configuration

A Clavister Security Gateway configuration is nothing more complicated then a plain text-file. Each configuration section is a block of text starting with the name of the section, RULES, for instance, and ending with the END keyword. Each configuration item is a line of text within the configuration section text block. Comment lines begin with a hash character (#).
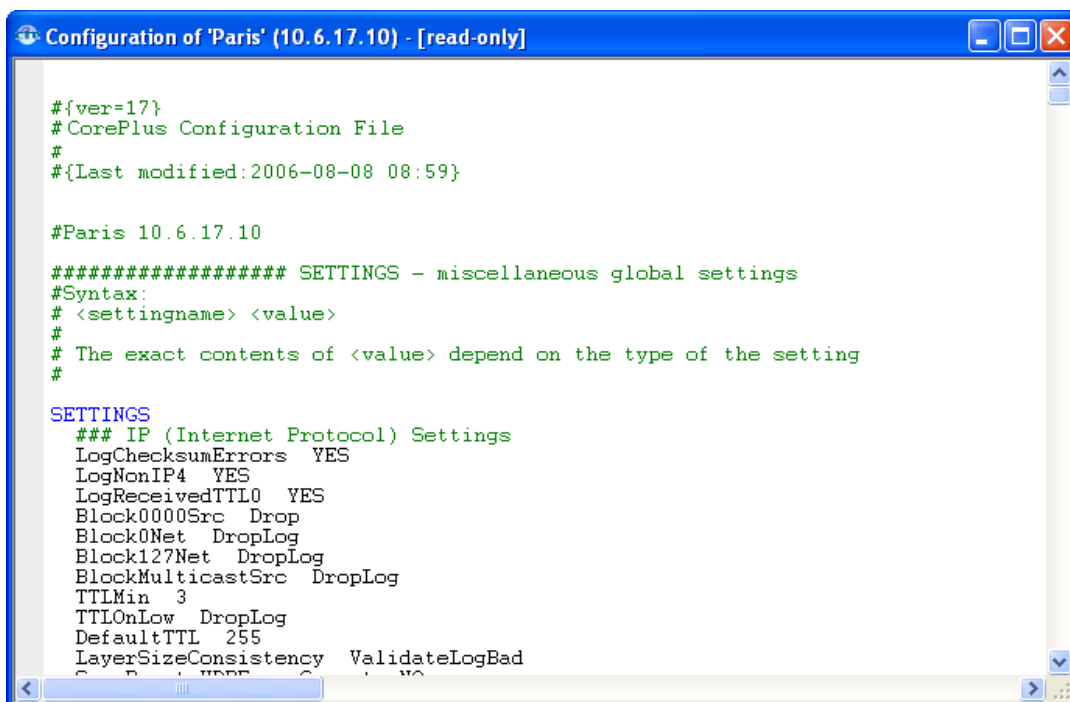
Below is an extract of a gateway configuration file. The extract shows the routing table for the gateway.

```
################## ROUTES - Routing table
#Syntax:
#
#
ROUTES
# if1net network routed via "if1"
if1  if1net 0.0.0.0
# if2net network routed via "if2"
if2  if2net 0.0.0.0
# if3net network routed via "if3"
if3  if3net 0.0.0.0
# Default route
if1  all-nets  10.4.0.1
END
```

The Security Editor parses the configuration text-file, and presents a "graphical" representation of the configuration sections and items. In some cases though, the Security Editor is unable to parse the configuration file. This might happen, for instance, when the configuration file contains unknown sections or corrupted data.

When the file cannot be parsed, the Security Editor will set the status of the gateway to "Configuration error(s)", add a red error symbol to the gateway icon, and refuse to expand this node in the tree view. In such an event, the configuration file needs to be edited in text-mode to be able to correct the error. FineTune includes a text-mode configuration editor for this purpose. To launch the editor, first select a gateway, and then choose **Edit Configuration** in Text-mode from the **Edit** menu in the Security Editor. The editor will be displayed with the gateways configuration in text-mode, similar to the screen shot shown below.

The text-mode editor uses the same concept of checking out and in configurations as the Security Editor. This means that the configuration is opened in read-only mode. The editor will automatically try to check out the configuration when any editing is performed. It's possible to validate the configuration before saving by taking **Validate** from the **File** menu. Save and check in the configuration by closing the text-mode editor.

Note

*The Security Editor will not automatically re-parse a gateway configuration that has been modified using the text-mode editor. This has to be done manually, by right-clicking the gateway and choosing **Get Latest Version** from the **Version Control** sub-menu.*

2.11. Boot Media Operations

When installing a product from the Clavister Security Gateway software series (ie. on non-Clavister hardware), the "New Security Gateway" wizard will generate a boot media that can be used for non-Clavister hardware. The boot media contains the CorePlus firmware, remote management encryption keys and a number of configuration files. The boot media chosen is ideally a burnable CD-ROM since this has sufficient capacity for all files. If an older style floppy disk is used then only the *mini-core* will fit on this.

In some cases, the boot media might need to be re-written. One reason can be, for instance, that the media has been damaged. The **Boot Media** submenu available from the **Action** menu in the Security Editor contains the following boot media related commands.

Action: *Save to Boot Media*

Brings up a boot media wizard that saves the selected gateway's most recent configuration and the remote management keys to a Clavister Security Gateway boot media. The file *FWCore.cfg* on the boot media is also copied to *FWCore_O.cfg*. If the wizard determines that the media is not a ´Clavister Security Gateway boot media, it will prompt to create one, producing the same results as the **Create Boot Media** command outlined below.

Action: *Create Boot Media*

The **Create Boot Media** command will bring up a boot media wizard that generates a complete boot media, similar to what is done in the New Security Gateway wizard.

Action: *Load Remote Management Keys*

Copies the remote management keys from a Clavister Security Gateway boot media to a specified gateway in the Management Data Source. This command can be used, for example, when manually restoring the Management Data Source after unintentional deletion of a gateway. It can also be used to transfer a gateway from one Management Data Source to another. It's recommended, however, that new remote encryption keys should be generated in any new Management Data Source and that these keys are saved to the Clavister Security Gateway boot media. This is to avoid the possibility of accidental double administration of a single gateway. For more information see Section 3.2.1, "Changing Remote Management Keys".

Chapter 3. Remote Management

3.1. Remote Management

All remote management of Clavister Security Gateways, including configuration, monitoring and even complete upgrades is secured through 128-bit encryption and authentication. The protocol used for the remote management is called *NetCon*, and is based on the CAST128 encryption algorithm. The NetCon protocol uses TCP and UDP as transport protocol, destination port 999.

NetCon uses a pair of pre-shared keys for authentication. These *Remote Management Keys* are unique for each Clavister Security Gateway, and are generated using a strong cryptographic number generator when new gateways are created in the Security Editor. The remote management keys are stored in the management data source.

A Clavister Security Gateway Appliance product is using *default* remote management keys during the initial setup. When FineTune has succeeded connecting to the Clavister Security Gateway, the keys will automatically be exchanged.

To gain permission to remotely administer a Clavister Security Gateway, three requirements have to be met:

1. The Remote Management Keys of the gateway have to be known.

2. The computer running FineTune has to belong to a network that has been granted administration rights.

3. The NetCon connections from FineTune to the Clavister Security Gateway have to be received on a specific interface on the gateway.

3.2. Administering Keys and Passwords

3.2.1. Changing Remote Management Keys

FineTune can be instructed to generate a new pair of remote management keys for a Clavister Secur-
ity Gateway, and make sure the new key pair is being used. To generate new keys, first select the
target gateway in the tree view of the Security Editor, and then choose **Change Remote Manage-
ment Keys...** from the **Action > Communication** menu. *The communication wizard* is used in the
same way as in the Section 3.3.1, "Uploading a configuration" section.

3.2.2. Reverting to Default Remote Management Keys

A Clavister Security Gateway can be reset to its factory default settings using an option in the boot
menu available from the local console of the Clavister Security Gateway. If this has been done, the
gateway will be using the default remote management keys that were originally shipped with the
product. As the Management Data Source still contains the keys used before the reset, FineTune will
be unable to communicate with the gateway.

This can be solved by reverting the remote management keys in the Management Data Source to the
default keys. To revert to default keys, first select the target gateway in the tree view of the Security
Editor, and then choose **Revert to Default Remote Management Keys...** from the **Action > Com-
munication** menu. *The communication wizard* is used in the same way as in Section 3.3.1,
"Uploading a configuration".

> ### Note
> *When the keys have been reverted and communication with the Clavister Security
> Gateway has been re-established, new keys should be generated immediately to min-
> imize the risk of an unauthorized administrator taking control. (See Section 3.2.1,
> "Changing Remote Management Keys" above).*

3.2.3. Changing the Gateway Password

The local console of the Clavister Security Gateway can be protected by a password to prevent tam-
pering. The password can be set initially from the New Security Gateway wizard, but can also be set
later using the *change security gateway password* command.

> ### Note
> *This password is only used from the local console on a Clavister Security Gateway.*

3.3. Uploading and Downloading Configurations

3.3.1. Uploading a configuration

A gateway configuration can be uploaded to a running Clavister Security Gateway at any time. To upload a configuration, first select the target gateway in the tree view of the Security Editor, and then choose **Upload Configuration...** from the **Action > Communication** menu.

A communication wizard similar to the one below will be displayed. The Clavister Security Gateway that was selected in the tree view will automatically be marked with a check box. Additional gateways can be selected or de-selected by clicking the corresponding check boxes.

If the **Automatically activate uploaded configurations** option is selected, the Clavister Security Gateways will activate the new configurations as soon as they have been received.

> ### *Committing IPsec Changes*
> *The adminstrator should be aware that if any changes that effect the configurations of live IPsec tunnels are committed, then those live tunnels connections WILL BE TER-MINATED and must be re-established.*

Click the **Next** button to start the upload. The *most recent* configuration will be uploaded to all selected Clavister Security Gateways.
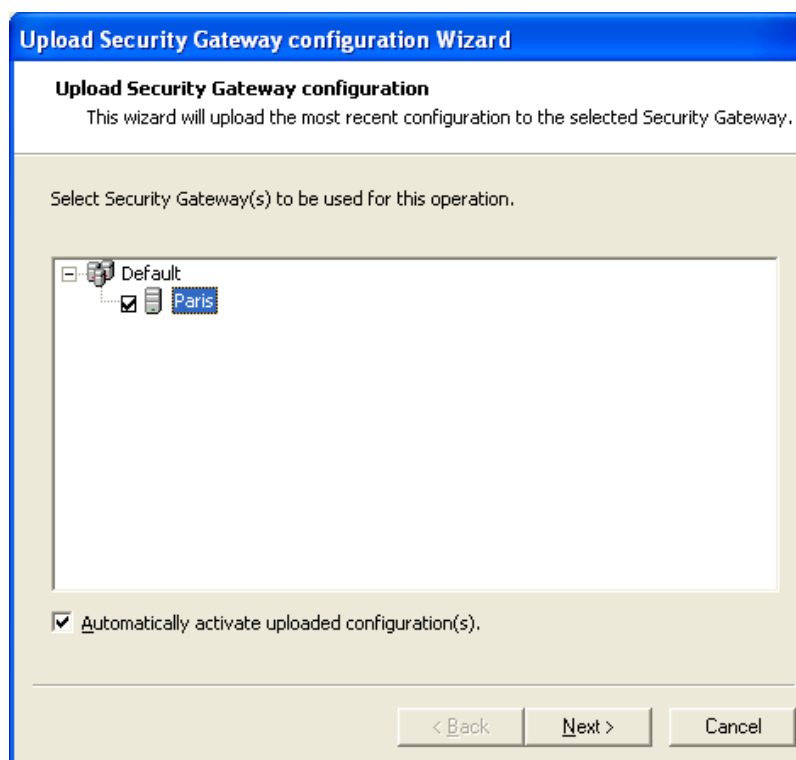
The next wizard page will display a list containing all the Clavister Security Gateways that configurations are being uploaded to, along with the status of each upload. Click the **Properties...** button to display an Event Properties dialog box where a detailed log of the progress is listed.

After a new configuration is activated, a fail-safe test is performed to verify that the Clavister Security Gateway can still be reached from FineTune. If the test fails, the gateway will automatically revert to its previous configuration. In this way, an administrator is prevented to lock himself out from a remote gateway.

The previous configuration version is also used if the new configuration contains information that

cannot be parsed by the CorePlus. The Event Properties dialog box will then contain an error log.

When a new configuration has been activated successfully, a text similar to the following is displayed in the Event Properties dialog box:

```
Attempting to connect to the Security Gateway.
Uploading to Security Gateway.
Upload successful.
Re-reading configuration.
Waiting for answer from Security Gateway.
Configuring from FWCore_N.cfg.
Configuration done.
Configuration "FWCore_N.cfg" (v21) verified for bi-directional
communication
```

3.3.2. Deploying a configuration

The **Deploy Configuration** command, available in the **Action** menu of the Security Editor, is similar to the Upload Configuration command, with one major difference; Deploy Configuration will automatically select gateway that have configurations that are more recent in the data source. These gateways are also displayed in the Security Editor with the status **Needs Deployment**.

3.3.3. Downloading a configuration

The running configuration may be downloaded from a Clavister Security Gateway and stored in the management data source. To download a configuration, first select the target gateway in the tree view of the Security Editor, and then choose **Download Configuration ...** from the **Action > Communication** menu. *The communication wizard* is used in the same way as in the Section 3.3.1, "Uploading a configuration" section above.

The version number of the downloaded configuration will be the version number of the most recent configuration in the management data source increased by 1, *or* the version number of the running gateway configuration, whichever is highest.

For example, if the running gateway configuration has version number 10 and the most recent version in the management data source has version number 7, then the version number of the downloaded configuration will be 10. On the contrary, if the running gateway configuration has version number 5 and the most recent version in the management data source has version number 7, then the version number of the downloaded configuration will be 8.

3.3.4. Re-reading a configuration

A Clavister Security Gateway can be instructed to re-read its configuration, meaning that the gateway reads its current configuration and performs the same initialization procedures as it does upon start. To perform a configuration re-read, first select the target gateway in the tree view of the Security Editor, and then choose **Re-read Configuration...** from the **Action->Communication** menu. *The communication wizard* is used in the same way as in the Section 3.3.1, "Uploading a configuration" section above.

3.3.5. Restarting a Clavister Security Gateway

A Clavister Security Gateway can be instructed to perform a complete restart, similar to a power off/power on operation. To perform a Clavister Security Gateway restart, first select the target gateway in the tree view of the Security Editor, and then choose **Restart Security Gateway..** from the **Action->Communication** menu. *The communication wizard* is used in the same way as in the Section 3.3.1, "Uploading a configuration" section above.

3.4. Upgrading CorePlus

Complete software upgrades of the CorePlus can be performed remotely and securely using the Net-Con protocol which is the Clavister protocol used for communication between FineTune and Clavister Security Gateways. There are two options for upgrades, *CorePlus core* upgrades and *CorePlus loader* upgrades.

3.4.1. Upgrading the CorePlus core

A core is a complete build of the CorePlus network operating system, containing all code necessary for the functioning of the Clavister Security Gateway. Whenever new functionality is added to CorePlus, or when problems have been found and corrected, a new core is produced. The new core is packaged, digitally signed and made available for download on the Clavister Client Web Pages at https://clientweb.clavister.com.

There are two types of core upgrades:

- Minor upgrades

- Major upgrades

These are defined in the Clavister End User License Agreement which is found in the accompanying license agreement file on the CD-ROM.

The highest core version that is permitted to run is determined by the particular License purchased from Clavister.

Warning
make sure you use the correct core for your hardware type.

When downloading and unpacking a core upgrade package on the server or workstation running FineTune, the actual Clavister Security Gateway core will be placed in a pre-defined directory. This directory is specified in the *File Locations* tab of the **Options** dialog box that is displayed by choosing **Options...** from the **Tools** menu. The default setting for this a directory called **Cores** in the installation directory.

To upload a new core to a Clavister Security Gateway, first select the target gateway in the tree view of the Security Editor, and then choose **Upgrade > Security Gateway Core...** from the **Action > Communication** menu. *The communication wizard* is used in the same way as in the **Uploading a configuration** section.

The second page of the communication wizard will be similar to the sample shown below. This page lists all cores available in the *Cores* directory. The first column lists the name of the core file. The second column displays the core version and the third column displays the date the core was created.
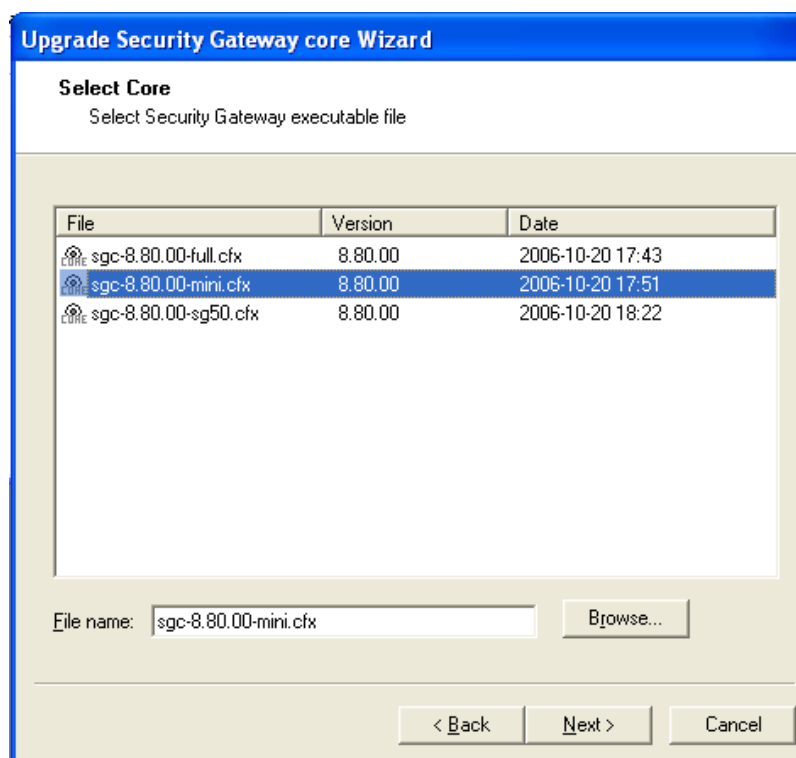
Select the core that should be uploaded to the Clavister Security Gateway and click the **Next** button.
If the required core is not shown in the list, the **Browse...** button can be used to browse the file sys-
tem for a core in another location.

When the core has been uploaded, the Clavister Security Gateway will perform a shutdown and then
start the new core.

Note
*All open connections through the Clavister Security Gateway will be dropped when the
gateway is upgraded with a new core.*

3.4.2. Upgrading the CorePlus loader

The CorePlus loader is the base software module used to operate a Clavister Security Gateway. This
loader takes care of initial bootstrap functions when the hardware is switched on such as boot sector
code reading, memory and file management, RS-232 console driver loading and so on. It is applic-
able to Clavister Security Gateways based on both Clavister and non-Clavister hardware.

Upgrading the CorePlus loader is rarely required. If it is, then it will be associated with a new ver-
sion of the CorePlus operating system and will be discussed in the release notes for that version
along with instructions for how to upgrade.

The upgrade operation is similar to the CorePlus core upgrade procedure. First select the target
Clavister Security Gateway in the tree view of the Security Editor, and then choose **Upgrade >
Loader...** from the **Action > Communication** menu. *The communication wizard* is used in the same
way as in Section 3.3.1, "Uploading a configuration".

Chapter 4. Licenses

4.1. The Clavister Security Gateway License

Each installed Clavister gateway requires a *Clavister Security Gateway License* in order to function. The license serves several purposes, including regulating the functionality of the gateway and protecting against unauthorized use of Clavister products.

A Clavister Security Gateway without a license will operate in *demonstration* mode only, meaning that the gateway will cease to function after two hours of operation. A restart is then required to continue running the product for another two hours.

Clavister provides a secured web site, the Clavister Client Web, where all licenses can be administered. Furthermore, Clavister FineTune includes all functionality needed for license management.

All Clavister products are shipped *without* a license. However, a printed *Certificate of Authenticity* is included with the packaged product. This Certificate includes a *registration key* which is used to register the purchased product. The registration is automated from within Clavister FineTune, but it can also be performed manually on the Clavister Client Web. When the registration is completed, a license is automatically generated and deployed to the installed Clavister Security Gateway.
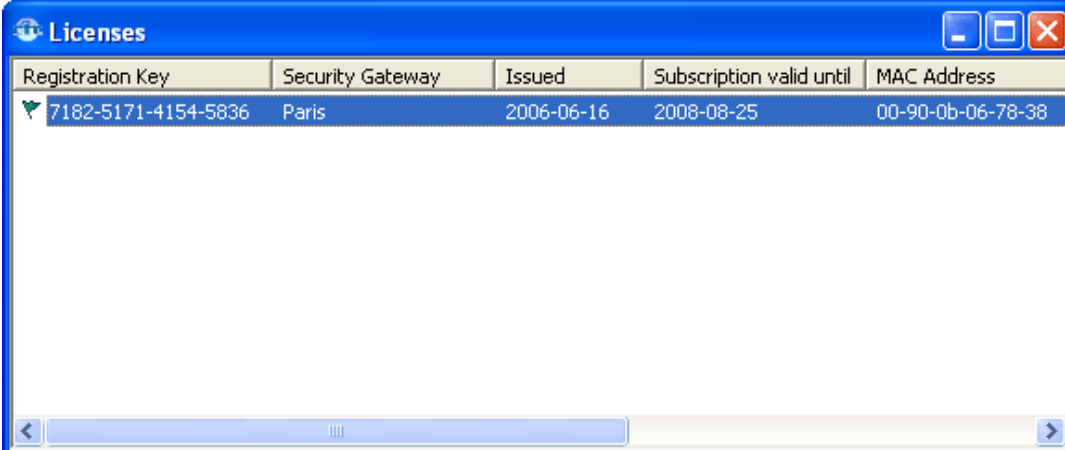
The license itself is a file that is stored in the management data source. When the license is uploaded to the Clavister Security Gateway, it is stored as license.lic on the gateway's boot media. The license is bound to the actual gateway hardware using the *MAC address* of one of the Ethernet adapters in the hardware.

FineTune provides several tools for managing licenses. The Registration wizard is used to register a newly installed Clavister Security Gateway. The wizard will collect all necessary information from the Clavister Security Gateway, contact the Clavister Client Web, automatically fetch a license and deploy it to the gateway. Please see Section 1.3, "Registering a Clavister license". Another important tool is the License tool, which provides functionality to administer all gateway licenses in the Management Data Source.

4.2. License Tool

The License tool shows all licenses currently available. A license file is stored in a sub-directory called **Licenses** in the same data source directory where the gateway that it is bound to resides. The license tool is opened by choosing **Licenses** from the **Tools** menu.

Figure 4.1. The License Tool

The following columns are shown in the license tool:

- **Registration key** - The registration key of this license. This number is found on the *Certificate of Authenticity*.

- **gateway** - The name of the gateway that the license is bound to.

- **Issued** - The date when the license was issued.

- **Subscription valid until** - The date until which you are allowed to download updates.

- **MAC Address** - The MAC address to which the license is attached.

- **IDP Subscription** - The date until which you are allowed to download IDP updates.

- **Anti Virus Subscription** - The date until which you are allowed to download Anti Virus updates.

- **Web Content Filter Subscription** - The date until which you are allowed to use Web Content Filtering.

4.2.1. License Properties

Clicking on **Properties** icon, or choosing **Properties** from the **File** menu, will show the following dialog:
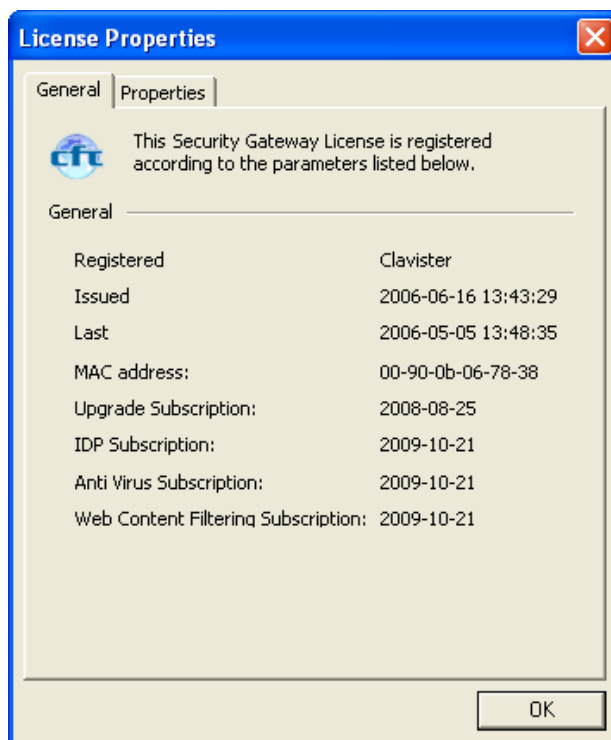
- **Registered** - The name of the customer of which this license is registered to.

- **Issued** - The date when the license was issued.

- **Last** - The date when the license was last modified.

- **Description** - Specifies the type of product this license is issued for.

- **MAC address** - The MAC address to which the license is bound.

- **Upgrade Subscription** - The date until which you are allowed to download updates.

- **IDP Subscription** - The date until which you are allowed to download IDP updates.

- **Anti Virus Subscription** - The date until which you are allowed to download Anti Virus updates.

- **Web Content Filtering Subscription** - The date until which you are allowed to use Web Content Filtering.

The **Properties** tab will show a list of all properties found in the license.

4.2.2. Communication Properties

In order to provide secure communication between FineTune and the Clavister Client Web, all traffic is sent over the Internet using Secure Socket Layer, SSL. If necessary, proxy servers can be specified to allow outgoing communication.

The communcation settings can be altered in the *Communication* page of the *Options* dialog box. Open the dialog box by choosing **Options...** from the **Tools** menu.
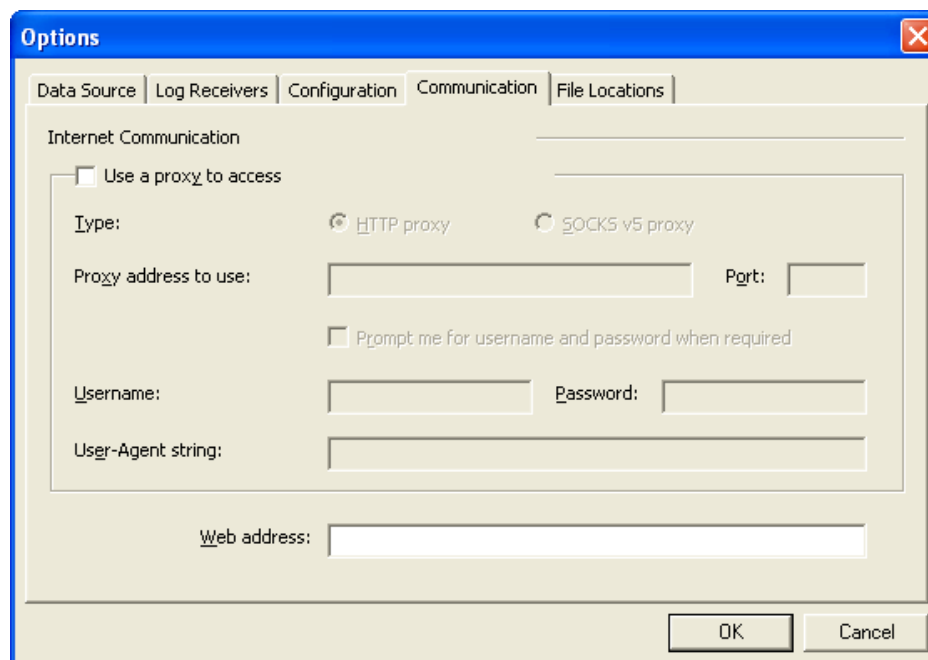
Two kinds of proxy servers are supported: HTTP proxy and SOCKS v5 proxy. If a HTTP proxy server is configured to only allow connections that use a certain user-agent, this can also be specified here. An example of this is proxy servers that are configured to only allow specific browsers to access the Internet.

If a proxy server requires a username and password, these can be entered here. As this information is stored in the registry, some users might feel uncomfortable storing such data in plaintext. Therefore, a checkbox called **Prompt me for a username and password when required** exists. If this checkbox is checked, the user instead will be prompted for a username and password when the connection to the Clavister Client Web takes place.

The address of the Clavister Client Web can also be specified here. It is set to *client-web.clavister.com* by default, and should not be edited.

4.2.3. Importing a license file

A license file can be imported to FineTune if needed, for instance, if the license was manually downloaded from the Clavister Client Web.
Follow these steps:

1.   Open the license tool from the menu **Tools** menu.

2.   Choose **Import...** from the **File** menu.

3.   Choose the directory where the license file is located, and press OK.

All valid license files found in this directory will now be imported into FineTune. If more than one data source is activated, a dialog asking to which data source the license file should be imported is presented. After choosing the destination data source, the license file is copied to this directory.

If a license file already exists with the same name in the target directory, a dialog will be presented, asking if this license file should be replaced with the one being imported.

Choosing the first option will replace the old license file this new license file. The old license file will be renamed to use the file extension .bak, instead of .lic.

Choosing the second option will leave the original license file intact, and cancelling the import procedure.
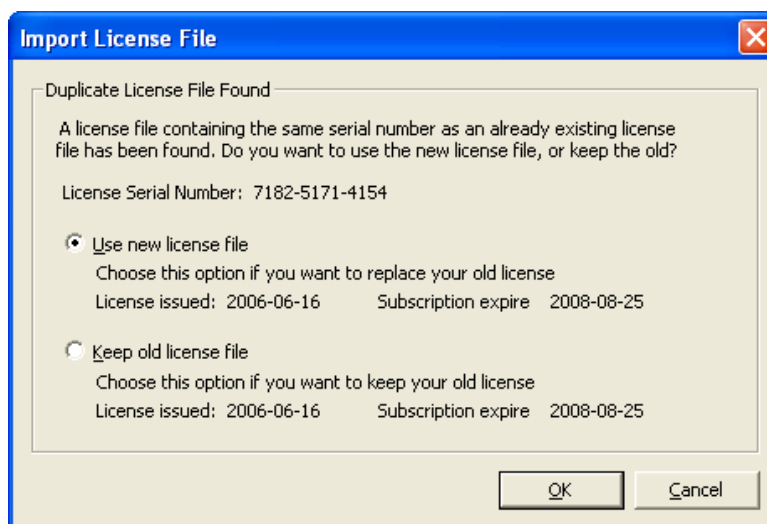
4.2.4. Binding license file to a Security Gateway

A license that has been manually imported in FineTune needs to be bound to a gateway. This is done by first selecting the actual license, and then choosing **Bind...** from the **License** > **Advanced** menu.

Choose the gateway to which the license file should be bound. Note that in order for this gateway to make use of the license file, an Ethernet adapter with the same MAC address as the one specified in the license file *must* exist.

If the **Upload license to gateway** checkbox is checked, FineTune will attempt to upload the license file to the gateway after binding the license. If successful, the gateway will re-read it's configuration in order to activate the new license file.

A green flag will be shown in the license tool window to indicate that a license file is bound to a gateway.
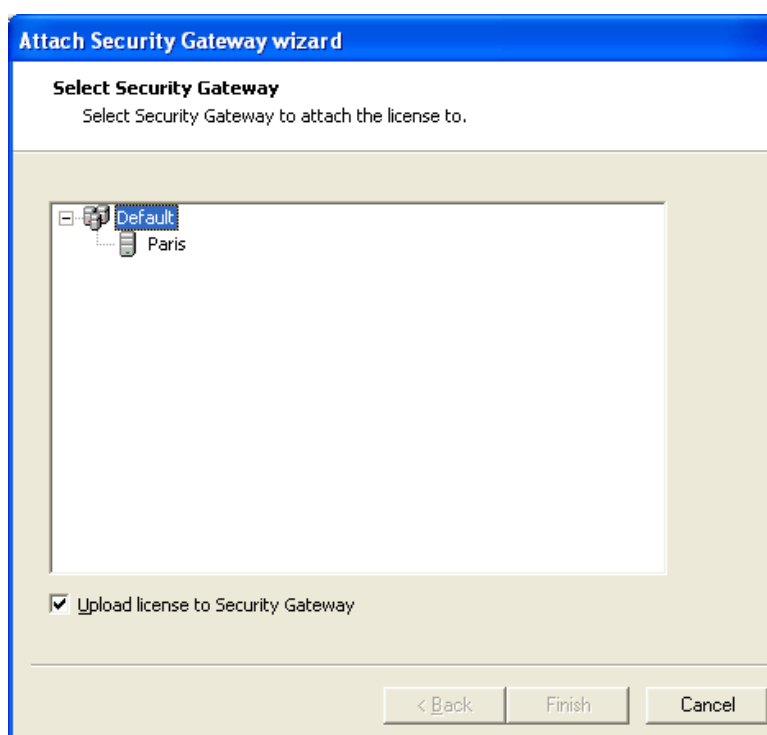
4.2.5. Unbinding a license file

If for some reason a license file must be unbound from a gateway (for example, the wrong gateway was selected, causing a MAC address mismatch), first select the license to be unbound, and then choose **Unbind** from the **License > Advanced** menu. A question will be presented, to make sure this is correct. Answering yes will unbind the license file from the gateway, removing the green flag in the license tool window.

> *Note*
> *The license file will still be stored on the actual gateway, and needs to be removed or replaced with a correct license file in order for the gateway to function correctly.*

4.2.6. Check for updates

FineTune can query the Clavister Client Web to check if an updated license is available. This is necessary, for instance, if the software subscription agreement has been renewed for an additional period of time. First, select a license in the License tool, and then choose **Check for updates...** from the **License** menu. It is also possible to do this in the Security Editor, selecting the gateway that the license file is bound to, and choosing the **Check for updates** item from the **Action > License** menu. A dialog box similar to the one to below will be shown:

The Clavister Client Web username and password have to be entered in this dialog box if not previously stored in the Windows Registry.

When clicking on the **Next** button the necessary information is sent to the Clavister Client Web. If a more recent license file is available, the new license will be fetched. A dialog will appear, asking if the new license file should replace the old.

Choosing yes will overwrite the old license file with the new. A new question will appear, asking if the license file should be uploaded to the gateway immediately. Pressing **Yes** will upload the license file to the gateway, which will re-read its configuration in order to activate the new license file.

4.2.7. Uploading a license file

A license can be uploaded to a Clavister Security Gateway at any time. Select the actual license in

the license tool and choose **Upload license...** from the **License** menu. It is also possible to do this from the Security Editor by selecting a gateway and choosing **Upload license...** from the **Action > License** menu.

Chapter 5. Logging

5.1. Clavister Logger

The Clavister Logger runs as a service on a Microsoft Windows Server. The service receives UDP data from a Clavister Security Gateway default on port 999, but this can be changed.

The data is sorted and stored in a hierarchic structure, where each Clavister Security Gateway is represented by a single directory. The log files are in binary format for fast analysis.

As noted previously, log servers must be enabled before logging becomes active.

5.1.1. Installing Clavister Logger

Where to Install the Clavister Logger

FineTune is used as the user interface for all Clavister Logger operations, including configuration and analyzing log data. This means that the computer and the directory where Clavister Logger is installed has to be accessible via Windows file sharing from the management workstations meant to access its logs. Write permissions may be selectively applied on a per-user basis; only the "fwlogger.cfg" file needs to be writable by administrators meant to manage the log receiver.

> *Note*
> *The NetBIOS channel only has to be uni-directional, i.e. Clavister Logger can be installed on a server in a de-militarized zone, with the rule-set allowing access to NetBIOS file shares from internal networks.*

Installing the Service

Insert the Clavister Security Software CD into the computer from which the Clavister Logger is to be run, i.e. the machine to which Clavister Security Gateway is to send log data. The installation software will start automatically.

If the installation does not start automatically, select Run from the start menu and enter D:\launch.exe (where D: is the letter of your CD-ROM drive). You will be presented with a list of choices, one of which is the Clavister logger installation.

Select installation and follow the on-screen instructions. Once the installation is complete, the wizard will start the service automatically.

It is worth emphasizing that Clavister Logger, as is the case with all Windows services, cannot be installed through a network share, only on local hard drives. The reason is that services are typically run as local users with no means to access network resources.

5.1.2. Configuring Clavister Logger

Configuring Clavister Logger is done using FineTune.

All configuration settings are stored in file called fwlogger.cfg, residing in the installation directory

of Clavister Logger. This file is auto-generated with default settings upon installation of Clavister Logger, but has to be further configured using FineTune.

The file is not intended for manual editing.

Attaching to a Clavister Logger

Start FineTune and select **Tools** from the menu bar, then **Options...** This will bring a up a dialog window used for attaching to any number of Clavister Loggers. Initially, the list will be empty.
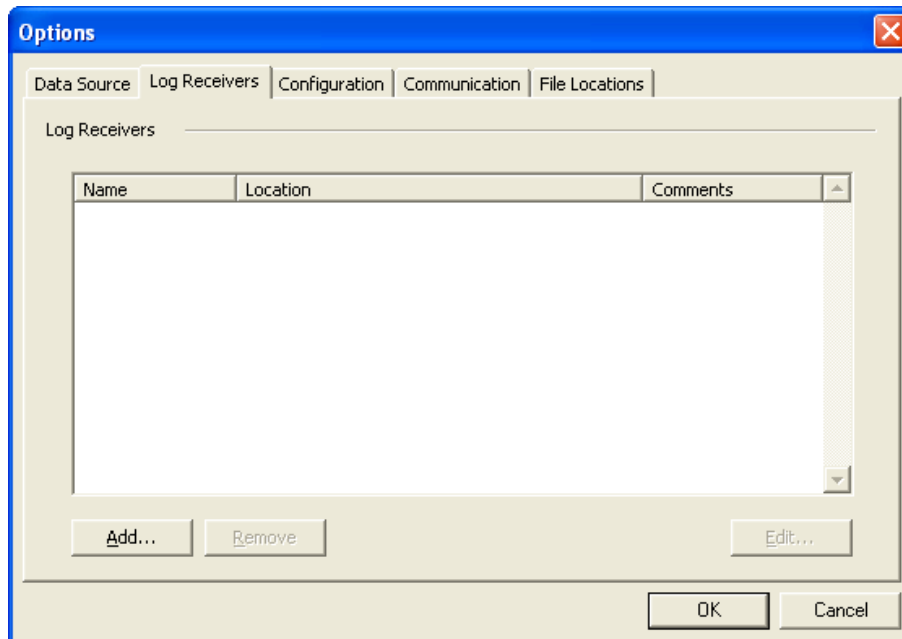
Click the **Add** button. In the Name field of the dialog window shown, enter a symbolic name for the new Clavister Logger.
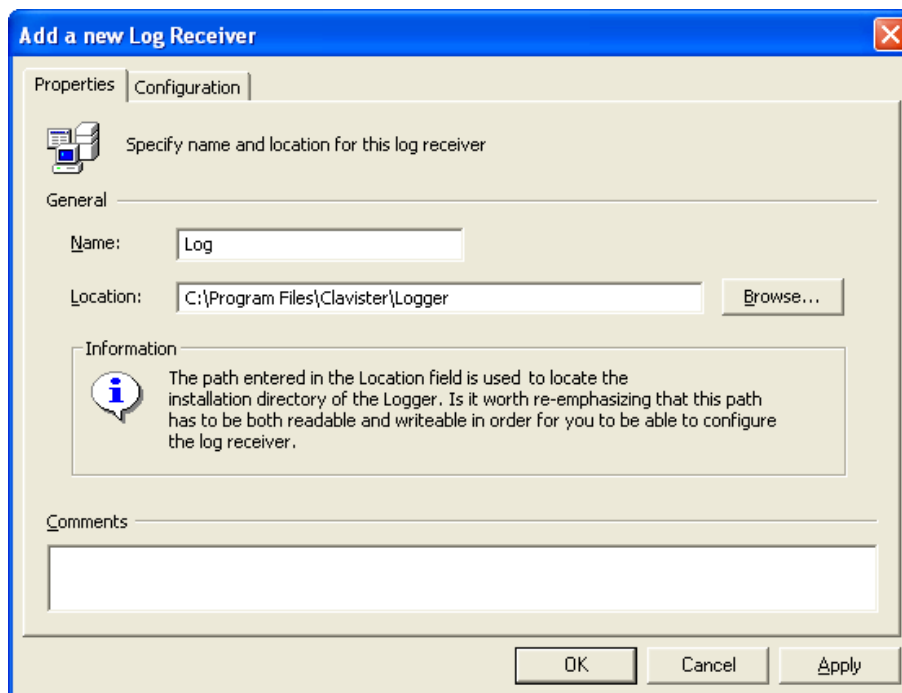
The path entered in the Location field is used by FineTune to locate the installation directory of the

Clavister Logger. It is worth re-emphasizing that this path has to be both readable and writeable in order for you to be able to configure the log receiver.

For instance, if the Clavister Logger is installed on a server named LOGSRV in a directory shared as FWLogger, the path entered would be \\LOGSRV\FWLogger. "X:\Directory" notation may of course be used as well, if the share has been previously mapped.

Configuring the Receiver

To avoid receiving unexpected or malicious log data, each Clavister Security Gateway that is configured to send log data to a Clavister Logger has to be specifically allowed in the configuration of that Clavister Logger.

Log data received from a Clavister Security Gateway that is not specified in the configuration will be rejected. Such attempts will be summarized in the event log of the server every 10 minutes.

In the list of connected receivers, select the Clavister Logger to be configured, then click the **Edit** button. The following dialog will appear:

The settings available in this dialog window directly affect the run-time behaviour of Clavister Logger. There is no need to restart the Clavister Logger after changing these settings, as the service continuously watches the configuration file for changes.
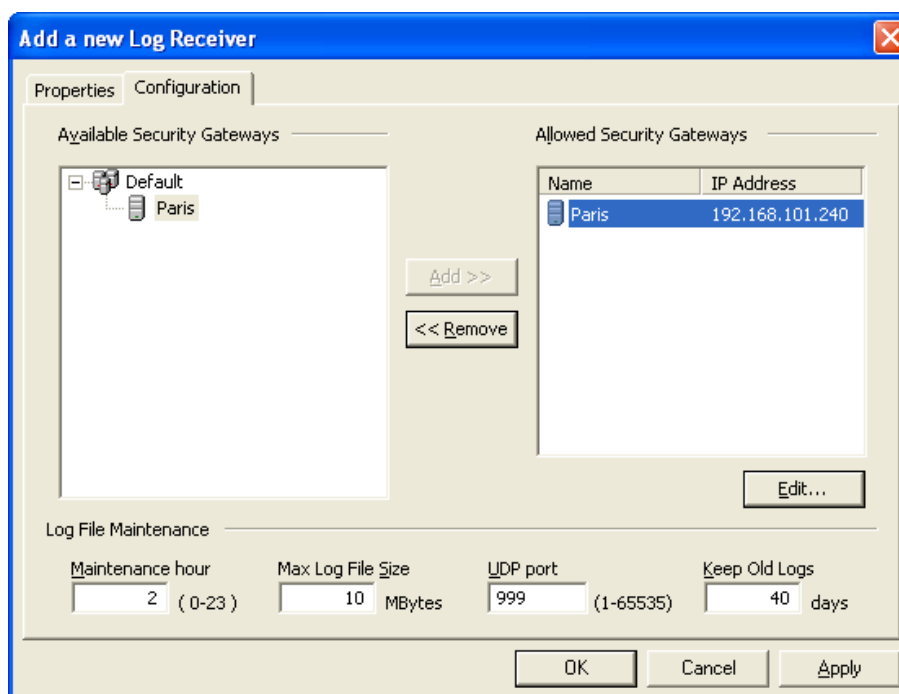
The upper right section of the dialog window controls what Clavister Security Gateways are accepted as log senders for this Clavister Logger. The list of **Available Security Gateways** displays all Clavister Security Gateways in the management database that have not already been allowed to speak to this particular Clavister Logger.

The list of **Allowed Security Gateways** contain all Clavister Security Gateways that are to be accepted by this Clavister Logger.

To assign an available Clavister Security Gateway to this Clavister Logger, select the gateway in the list of **Available Security Gateways** and click **Add**. To remove a gateway, select the gateway in the list of **Allowed Security Gateways** and click **Remove**.

> *Note*
> *Multiple selections are allowed in both the lists, Available Security Gateways and Allowed Security Gateways.*

If the sender IP-address used by the Clavister Security Gateway for communication with the management workstation differs from the address used for communication with the log receiver, you will need to change the IP address allowed to speak to the Clavister Logger. This is accomplished by double-clicking the entry in the Allowed Security Gateways list and editing its IP address in the resulting dialog. This also applies to gateways having their IP addresses changed
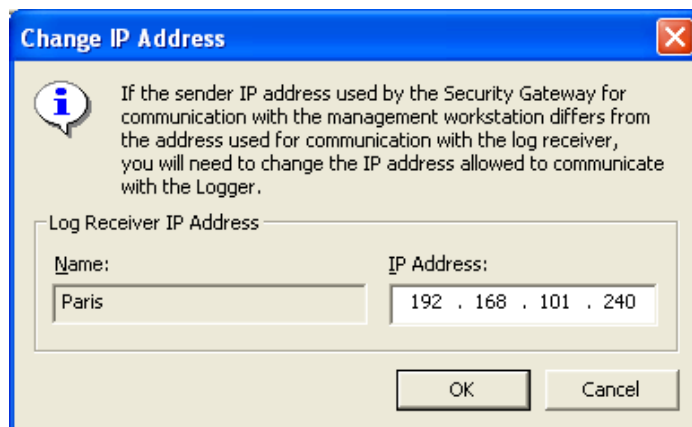
The Log File Maintenance section of the dialog window controls administrative functions of the Clavister Logger.

The **Maintenance hour** field indicates at what time the Clavister Logger should execute its maintenance tasks. These tasks include log file compression, removal of outdated log files, etc. The **Max Log File Size** field determines the maximum file size of a single log file. When a log file grows above this limit, it will be archived and replaced by an empty file. The **UDP Port** field indicates what port the logger should listen on, remember to use the same port in the logging gateway. The Clavister Logger will keep the log files for any number of days, specified by the **Keep Old Logs** setting. At the daily maintenance time, files older than the allowed limit will be deleted.

5.2. Log Analyzer

The log analyzer tool is an integrated utility in FineTune, used to perform fast searches and queries in the log data received by the Clavister Logger.

The tool gives you the ability to get an overview of Clavister Security Gateways events that have occurred during a specified period in a fast and simple way. Furthermore, there are filter functions that allow you to single out interesting events with respect to a number of parameters.

The analyzer tool is also equipped with an advanced packet analyzer which can be used to display and analyze the content of packets that cause the log events.

A query language called LQL, Clavister's adaptation of SQL, is used in order to make the analyzer tool as flexible as possible. The query language is very much similar to the SQL used for database queries, however with gateway specific details. A detailed reference of LQL can be found in Section 5.4, "LQL Reference". You may write LQL queries directly in the analyzer tool, but there is also an intuitive wizard that may be used for less advanced queries.

The log analyzer tool is activated from Log menu of FineTune

Select **Tools** from the menu bar, and then click **Log Analyzer**, or click on the **Log Analyzer** icon in the Tools.

This will bring up a window similar to the one shown below.
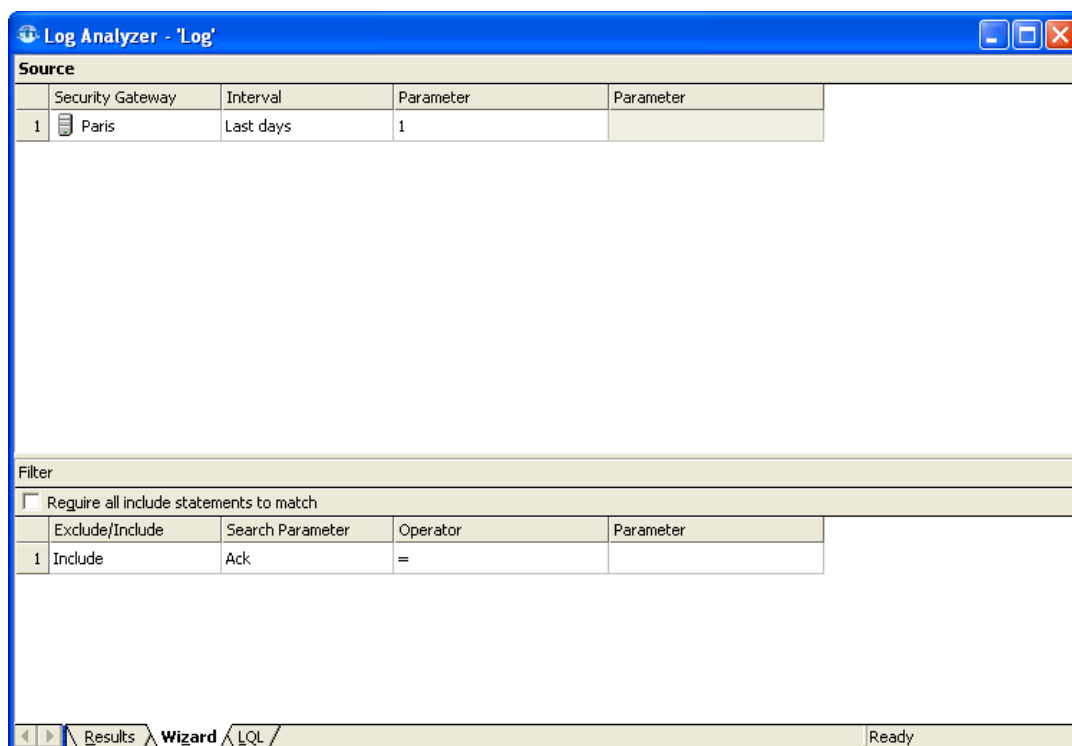
There are three tabs at the bottom of the window, used to switch between the three different views of the tool; the **Results** view, the **Wizard** view and the **LQL** view.

5.2.1. The Wizard View

The wizard is used to construct a log query in an easy way by selecting appropriate sources and filters in the drop-down menus. Additional rows are added automatically when entering data into the wizard.

Specifing Log Sources

The *source* section of the wizard specifies what Clavister Security Gateway to be queried and the time period for each gateway.
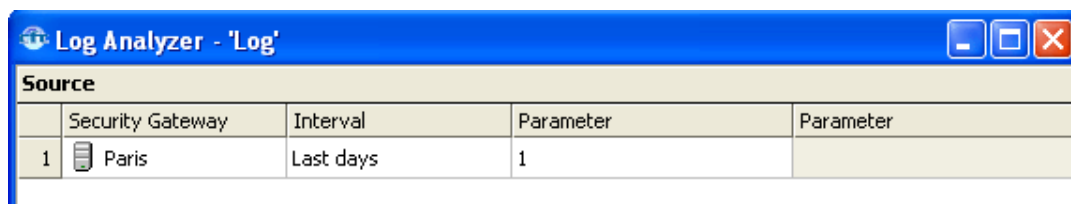

Select the Clavister Security Gateway you wish to query in the drop-down menu to the left. The menu will list all gateways specified as **Allowed Security Gateways** in the **Configure Receiver** section of the Clavister Logger configuration. It's possible to query all gateways by choosing **ALL** as gateway.

The drop-down in the middle gives four alternatives for specifying a time period:

- Selecting **Times** will allow you enter a date range in the two blank text boxes to the right. The dates have to be specified in the ISO standard format, yyyy-mm-dd HH:MM:SS, terminated at any point. For instance, the time-of-day part may be omitted, if you so wish.

- Selecting **Last days** will limit the log search to the last *n* days, where *n* is specified in the text box to the right.

- Selecting **Last full days** is similar to the above with the difference being that the search starts at the beginning of a day, and will only include events up to 23:59:59 yesterday.

- Selecting **Last hours** will limit the log search to the last *n* hours, where *n* is specified in the text box to the right.

- Selecting **Last full hours** is similar to the above, the difference being that the search starts at the beginning of an hour, much like the "full days" option.

Log data from several gateways may be queried simultaneously. This is done by adding more rows to the source section.

Specifing Event Filters

The *Filter* section provides functionality to include or exclude log entries that matches certain criteria.
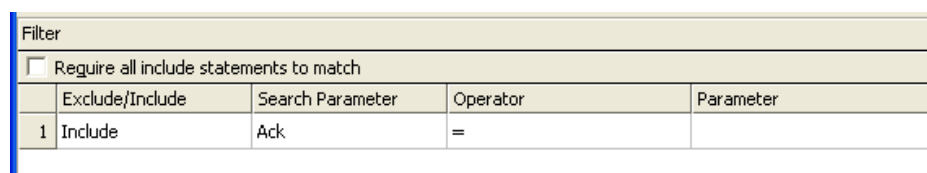
The drop-down menu on the left determines whether a log entry should be included or excluded if the criteria on the row are met. The second drop-down menu specifies the filtering parameter. For a detailed explanation of the different parameters, see the LQL Reference section. The third drop-down menu determines the operator to be used when filtering on the parameter specified above. The drop-down menu on the right is the specification for the criteria.

The query is executed by selecting **Run Query**, or by pressing **Ctrl-E**. If no syntax errors were encountered, the query process will start, with a window showing the progress of the search. When the search is finished, the **Results** view will automatically be shown.

The screenshot below show two different query samples:
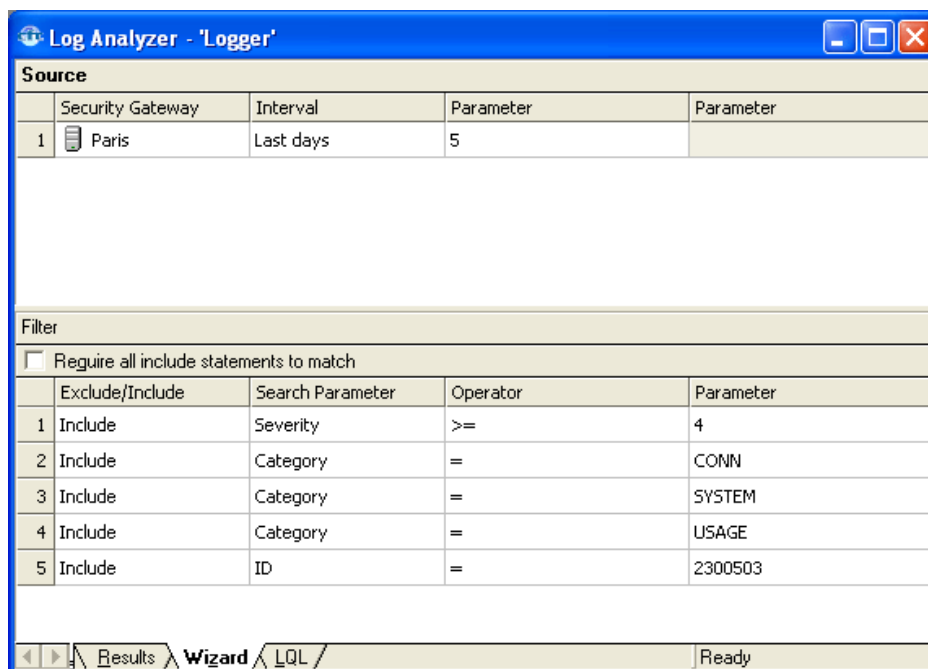
Sample query: The above settings will result in a query that will search the log files of the gateway for log events received during the last 5 days. The search will only include events that match the criteria specified in the screenshot.

5.2.2. The LQL View

The LQL view gives you the possibility to manually write queries using LQL. The biggest advantage of doing so, is that it is possible to construct much more advanced queries than by using the Wizard view.

As in the case of the Wizard view, the query is executed by selecting **Query** from the **Query > Run** menu in the menu bar, or by pressing **Ctrl-E**.

All previously executed queries are shown in the **Old LQL queries** section of the LQL view. This also includes queries generated by the Wizard view. You may re-use these queries by clicking on them with the right mouse button and selecting **Copy**. The query may then be pasted into the LQL query section.

Note
Queries created in the Wizard view may be viewed in the LQL view. Manually written queries in the LQL view however, can not be viewed in the Wizard view. When switching to the Wizard view, the settings of the last Wizard-generated query will be displayed.

5.2.3. The Results View

The Results view, as shown below, displays the result of the search. The view is divided into three sections, each with a different detail level and content.

The Results view is divided into three separate sections with different levels of detail. The upper-most section displays all log events that are part of the result from the search, sorted by date with the oldest event listed first.

Figure 5.1. The Results View - top section

The columns shown are, from left to right:

- **Date** and **Time** when the event was received by the log server and reflects the log server's time locale.

- **Device Time** is when the event took place according to the time locale of the gateway

- The **Name** of the Clavister Security Gateway where the event took place.

- **Message ID** - A unique identifier that identifies this event in the Log reference guide

- The name of the **Rule** that caused this log entry.

- **Category** of the event. Category is the top level of the event hierarchy. See section, Section 5.4, "LQL Reference", for a list of categories and descriptions.

- **Event** - The name of the event. For each event there might be a number of possible actions. Not all events have an action.

- **Action** - A typical action might be "Open" which could also occur with other events in other categories. Not all events have an Action.

- The **Source** of the packet causing the event. Depending on the type of packet, different source information is displayed:

  - For TCP or UDP packets: *interface, IP address and port*.

- • For other IP packets: *interface and IP address*.

- • For ARP packets: *interface and MAC address*.

• The **Destination** of the packet causing the event. The information displayed depends on the type of packet, as above.

• The **Protocol** of the packet causing the event.

By clicking on a specific event, the row will be highlighted, and the lower two sections of the view will display detailed information regarding the event.

Figure 5.2. The Results View - middle section

```
ID: 300049
Event: invalid_arp_sender_ip_address
Action: drop
Message: Failed to verify ARP sender IP address. Dropping
Rules
    Rule name: Block127Net
Ethernet Packet
    Sender: 000d:4827:005e
    Destination: ffff:ffff:ffff
    Protocol: ARP
Arp Packet
    Opcode: Request
    Hardware address space: Ethernet
    Protocol address space: 1
    Hardware address length: 6
    Protocol address length: 4
    ARP Packet Data
        HWAddr Sender: 000d:4827:005e
        HWAddr Destination: 0000:0000:0000
        Protocol Sender: 127.0.5.14
        Protocol Destination: 127.0.5.14
```

Detailed information regarding an event is displayed in the middle section of the result view. The information is shown using a tree display. More details can be retrieved by expanding the branches of the tree marked with a "plus" symbol.

If an event containing a packet dump, such as a DROP event, is selected in the top section of the results view, the bottom section shows a byte dump of the first 150 bytes of the packet causing the drop. The dump is displayed in hexa-decimal format.

Figure 5.3. The Results View - bottom section

```
000000  00 90 0B 01 EE 10 00 80 C8 57 D0 B2 08 00 45 00   .........W....E.
000010  00 28 4E 27 00 00 2F 06 BC 55 C0 A8 00 02 C0 A8   .(N'../..U......
000020  00 01 C7 AC 00 50 B5 88 00 03 44 81 3C 99 50 10   .....P....D.<.P.
000030  10 00 1F DE 00 00 00 00 00 00 00 00               ............
```

As mentioned in the beginning of this section, the results view may also be used to create further queries based on the result of a previous query.

This is done by right-clicking on a specific event in the top section of the view. The event chosen has to have source and destination information. In the menu shown, select **New Query** and select one of the alternatives in the sub-menu.

This will open up a new query tool, where a query is pre-entered with the address(es) selected, and a time frame encompassing one hour before and after the event that took place.

Color Settings

It is possible to color encode the output of the **Results** View to make it more easy to see what is dropped and so on. To get to the **Color Settings** choose **Color Settings...** from the **Edit** menu.
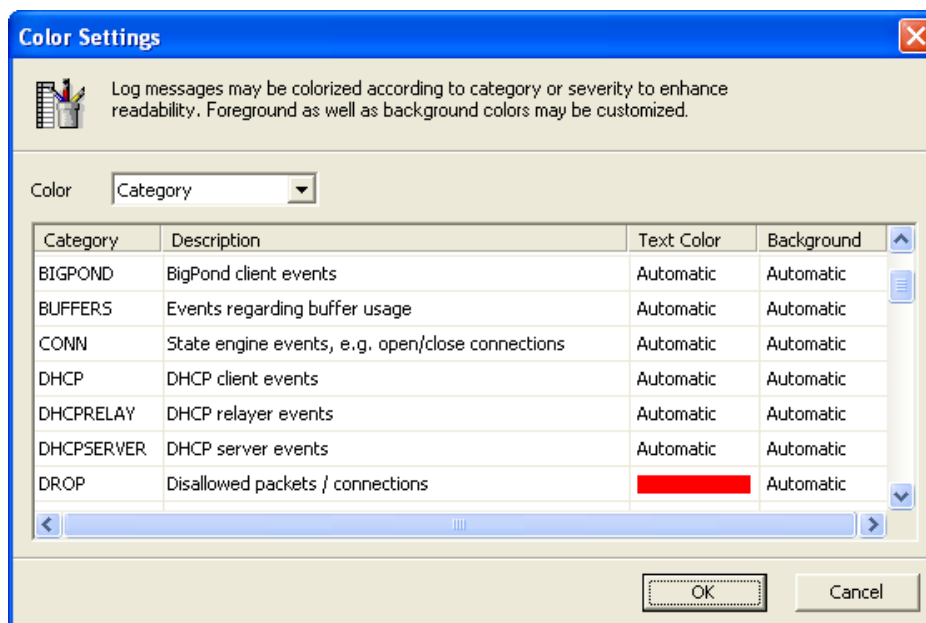
5.2.4. Export Log Data

It is possible to export logdata for use in other programs, or for sending to the support. This is done by choosing either **Selected Line(s)** or **All Lines** from the **File > Export** menu when in the *Results* view. It is possible to save the logdata in plain-text or binary format.
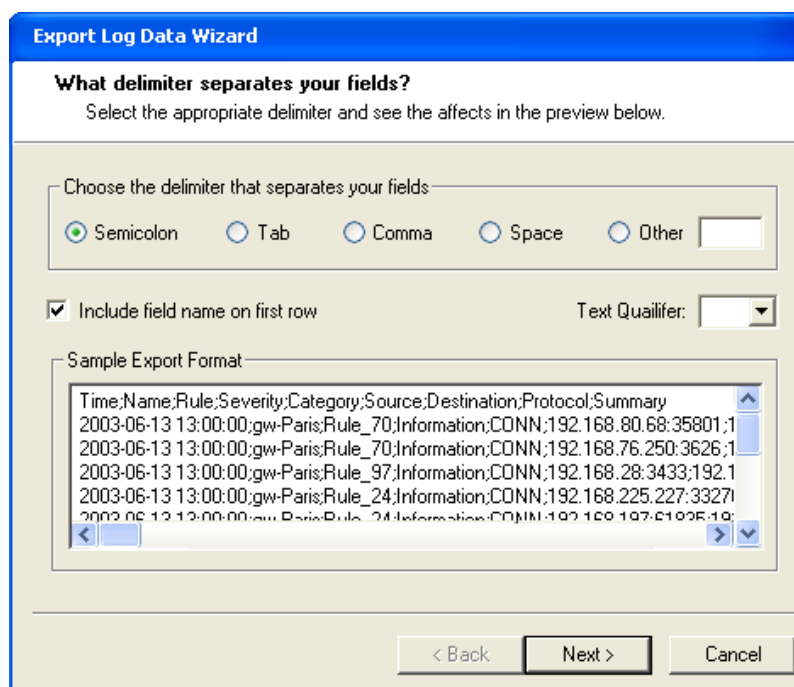
5.2.5. Log Utilities

The Log Utilities are small tools that can be used to run Whois, Ping, Traceroute and more on the

result of the query, these tools are useful to see where a connection came from, or what a certain port is used for.

5.3. Real-time log

FineTune is able to display log messages received from Clavister Security Gateways in real-time by selecting the desired gateway and choosing **Real-time Log** from the context menu.

This format of the log events presented in this log viewer is a hybrid of the Clavister Logger and SysLog formats: descriptive full sentences are displayed concerning the reason behind an event, but packet dumps and connection descriptions are logged in the syslog format.

The real-time viewer cannot display old log messages; only those that arrive while the log viewer is active are displayed.

The Real-Time Log Display communicates through the same encrypted connection that other remote management functions use. For this reason, FineTunes wanting to display real-time log data are not required to be listed as log receivers in the Loghosts configuration section.
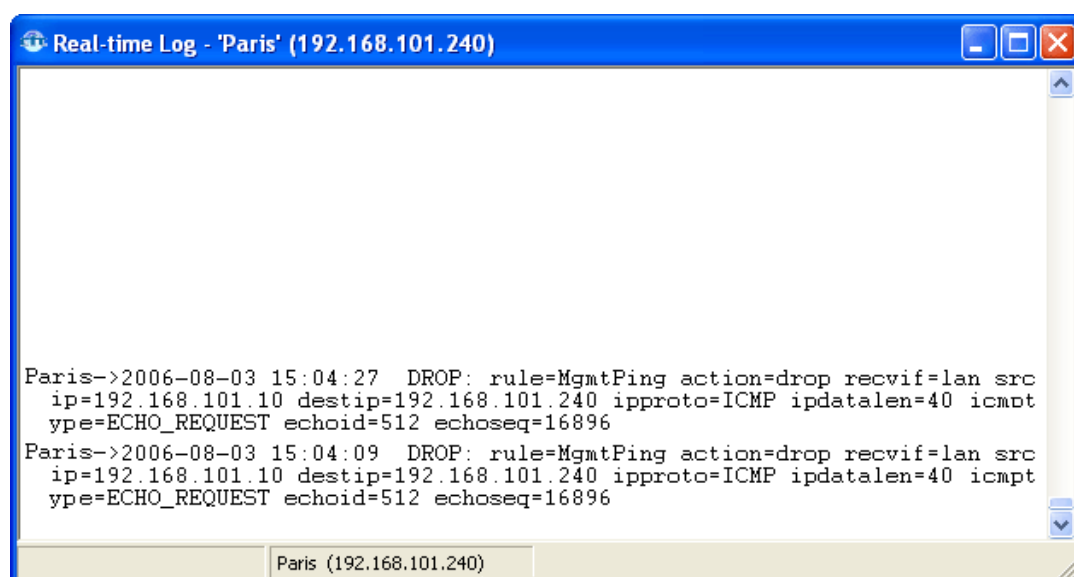
The output lines in the Real-time Log can be filtered by using the *Filter* tool. Right-click and select **Filter**.
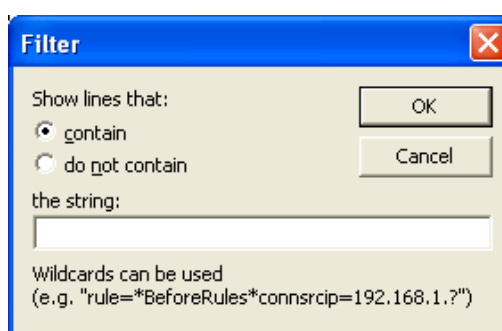
5.4. LQL Reference

LQL, Clavister Log Query Language, is the query language used to perform the log searches. In terms of format and syntax, LQL is very much similar to traditional SQL that is used as query language in database engines. Of course, LQL has a large number of Clavister Security Gateway specific keywords and statements.

The basic syntax of an LQL query is this:

SELECT <outputtype> [, <outputtype>]

FROM <gateway_and_time_statement>

[WHERE <logical_statement>]

Each LQL query is expected to start with the SELECT keyword

Directly after the SELECT keyword, one or more output types (see section Output types), separated by a comma, are specified. The integrated log analyzer expects raw binary data, so for queries in the LQL pane of the log viewer, use "SELECT BINARY".

After the FROM keyword, one or more gateway and time statements are specified.

Optionally, the WHERE keyword followed by a logical statement may be specified.

5.4.1. Logical operators

Logical operators are used to combine different LQL statements to form more complex statements. The following logical operators are defined in the LQL language:

Figure 5.4. Logical operators

Operator	Usage	Description
NOT	NOT Expression	Negates a Boolean expression.
AND	Expression1 AND Expression2	Combines two Boolean expressions and evaluates to TRUE when both expressions are TRUE.
OR	Expression1 OR Expression2	Combines two Boolean expressions and evaluates TRUE when either of the expressions are TRUE.

The logical operators are listed in precedence order; for example the 'OR' operator has a higher precedence then the 'AND' operator. By using parentheses to enclose parts of the statement the operator precedence can be changed.

Example 5.1. Using Logical Operators

srcip = '10.0.0.1' and (destip = '192.168.123.1' or destip = '192.168.123.2')

5.4.2. Comparison operators

Comparison operators are used to compare search variables with user specified values. The following operators are supported:

Figure 5.5. Comparison operators

Operator	Description
=	Equal to
>=	Greater than or equal to
<=	Less than or equal to
>	Greater than
<	Less than
IN	Range comparison

All user-specified values are expected to be quoted with ' chars.

Example 5.2. Using Comparison Operators

srcip = '10.0.0.1' and destip = '192.168.123.1'

srcip IN (10.0.0.1 - 10.0.0.255) and destip IN (192.168.123.1 - 192.168.123.255, 1.2.3.4)

5.4.3. Search variables

There are a number of predefined variables that can be used in the logical statements. The table below lists the variables currently defined.

Figure 5.6. Search variables

Variable	Value Type	Description
srcip	IPv4 address	Source IP address on the format: a.b.c.d
destip	IPv4 address	Destination IP address on the format: a.b.c.d
hwsrc	Ethernet address	Source ethernet address
hwdesc	Ethernet address	Destination ethernet address
severity	String	Log message severity
category	String	Category of the logged event. Example: SYSTEM, NETCON, USAGE, CONN, DROP
conn	String	Connection event. Example: Open, Close, Closing
srcport	Integer	Source port (0-65535)
destport	Integer	Destination port (0-65535)
ipproto	Integer	IP protocol (0-255 or name). Example: TCP, UDP, ICMP, 99
recviface	String	Receiving interface name. Example: ext, int, dmz
destiface	String	Destination interface name
icmptype	String	ICMP Message Type (0-255. Example: ECHO_REQUEST
arp	String	ARP opcode. Example: Request, Reply, Other
icmpsrcip	IPv4 address	Source IP address in ICMP-encapsulated IP packet
icmpdesctip	IPv4 address	Destination IP address in ICMP-encapsulated IP packet
icmpsrcport	Integer	Source port (0-65535) in ICMP-encapsulated IP packet
icmpdestport	Integer	Destination port (0-65535) in ICMP-encapsulated IP packet
icmpipproto	String	IP protocol (0-255) in ICMP-encapsulated IP packet
description	String	Description of the event
fin	Boolean	TCP FIN flag (0 or 1)
syn	Boolean	TCP SYN flag (0 or 1)
rst	Boolean	TCP RST flag (0 or 1)
psh	Boolean	TCP PSH flag (0 or 1)
ack	Boolean	TCP ACK flag (0 or 1)
urg	Boolean	TCP URG flag (0 or 1)

Variable	Value Type	Description
xmas	Boolean	TCP XMAS flag (0 or 1)
ymas	Boolean	TCP YMAS flag (0 or 1)
enetproto	Integer	Ethernet protocol number (0-65535)
rule	String	Rule name
satsrcrule	String	SAT source rule name
satdestrule	String	SAT destination rule name
enet[index]	Integer	Value at [index] bytes offset from the Ethernet header
ip[index]	Integer	Value at [index] bytes offset from the IP header
tcp[index]	Integer	Value at [index] bytes offset from the TCP header
udp[index]	Integer	Value at [index] bytes offset from the UDP header
algmod	String	Name of the ALG module that this log message originated from.
algsesid	Integer	ID of the ALG session that this log message originated from.
authrule	String	Userauth rule name.
authagent	String	Userauth agent. Example: http, xauth
authevent	String	Userauth event. Example: Login, Logout, Timedout, Disallowed
username	String	Username, from login/logout, as well as src/destusername
srcusername	String	The user that originated this connection/packet
destusername	String	The destination user

5.4.4. Output types

There are a number of output types defined that are used when specifying what data to be returned by the query.

All output types return data in plain text, except the binary type, which will return the data in a binary form used in the query tool. The binary output type is the only output type that is allowed when using the query analyzer tool, and it cannot be mixed with the plain text output types.

The following output types are defined:

Figure 5.7. Output types

Name	Description
binary	Binary form output, only used within the query tool.
srcip	Source IP address.
destip	Destination IP address
srcport	Source port
destport	Destination port
hwsrc	Source ethernet address
hwdest	Destination ethernet address
iphdrlen	IP header length
ipdatalen	IP data length
iptotlen	IP total length (data + header)
udpdatalen	UDP data length
udptotlen	UDP total data length
gateway	Name of the gateway that sent the data
time	The time when the event took place
recvif	Receiving interface
destiface	Destination interface
ttl	Time To Live field in the IP header

Name	Description
date	The date when the packet arrived at the logger
description	Description of the event
arp	ARP packet type
arphwdest	Destination hardware address in ARP events
arphwsrc	Source hardware address in ARP events
ipproto	IP protocol
icmptype	ICMP type
icmpsrcip	Source IP in an ICMP-encapsulated IP packet
icmpdestip	Destination IP in an ICMP-encapsulated IP packet
icmpsrcport	Source port of an ICMP-encapsulated UDP/TCP packet
icmpstd	ttl, icmptype, icmpipproto, icmpdestip, icmpsrcip and icmpdestport
tcpflags	All TCP flags
enetproto	Ethernet protocol
usage	Interface throughput
connusage	Connection statistics
rule	Name of the rule that this log entry matched
satsrcrule	Name of the SAT source rule that this entry matched
satdestrule	Name of the SAT destination rule that this entry matched
origsent	Amount of data sent by the originator (client end) of the connection
termsent	Amount of data sent by the terminator (server end) of the connection
conn	Conn event type
ack	TCP ACK flag (0 or 1)
fin	TCP FIN flag (0 or 1)
psh	TCP PSH flag (0 or 1)
rst	TCP RST flag (0 or 1)
syn	TCP SYN flag (0 or 1)
urg	TCP URG flag (0 or 1)
ece	TCP EXE flag (0 or 1)
cwr	TCP CWR flag (0 or 1)
category	Category of the logged event
tcphdrlen	TCP header length
tcpdatalen	TCP data length
tcptotlen	TCP total length (data + header)
standard	date, time, gateway, category, recvif, srcip, srcport, destip, destport, ipproto and description
tcpstd	tcpdatalen, tcphdrlen, fin, syn, rst, psh, ack, urg, ece and cwr
udpstd	udpdatalen
severity	Log message severity
algmod	Name of the ALG module that this log message originated from
algsesid	ID of the ALG session that this log message originated from
authrule	Name of the userauth rule applied
authagent	User authentication agent
authevent	User authentication event
username	Name of the user that logged in/out
usernames	username, srcusername, and destusername
srcusername	The user that originated this connection/packet
destusername	The destination user

5.4.5. Clavister Security Gateway statements

The gateway statement is used to specify the gateway or gateways to search for log events.

The syntax of a gateway statement is:

<gateway> [, <gateway>] [<time_statement>] [AND <gateway> [, <gateway>] [<time_statement>]]

5.4.6. Time statement

The time statement is used to specify a time interval for the data that is requested.

A time statement can be any of the following statements:

TIMES yyyy-mm-dd HH:MM:SS TO yyyy-mm-dd HH:MM:SS

LAST DAYS n

LAST FULL DAYS n

LAST HOURS n

LAST FULL HOURS n

(where n is any numerical value in the range from 1 to 1000)

If the TIMES statement is used, the date and time have to be specified in ISO standard format, as shown above, and may be terminated at any point, i.e. "TIMES 2000-01 TO 2000-02" is a valid time statement.

Chapter 6. Real-time Monitor

6.1. Overview

This chapter describes the real-time monitoring feature in FineTune. The real-time monitor is a tool for plotting real-time values from a gateway. The following tasks are possible using the Real-time Monitor:

- Monitor one or more systems concurrently

- Performance monitoring

- Bandwidth monitoring

6.2. Real-time Monitor Layout

The Real-time monitor is launched by clicking on the **Real-time Monitor** icon in the left-hand tool-bar in FineTune, or by choosing **Real-time Monitor** from the **Tools** menu.

A window similar to the one shown below will be displayed.

Figure 6.1. Real-time Monitor Layout
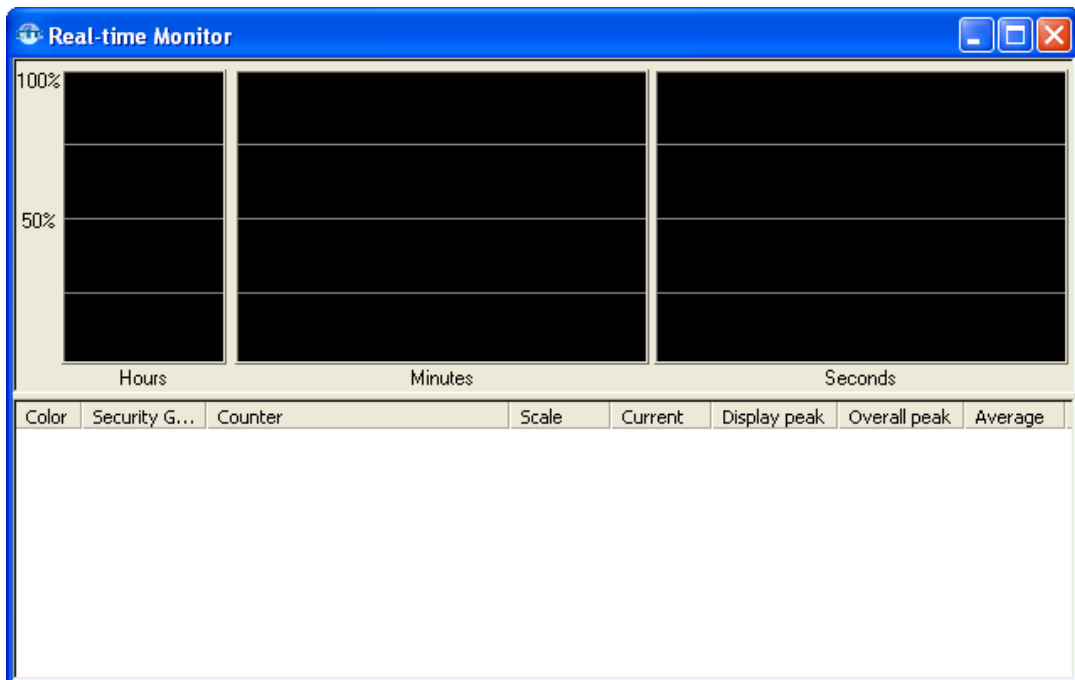
The diagram section of the display shows three diagrams side by side.

- The right-hand diagram shows statistics second by second.

- The center diagram shows average values minute by minute.

- The left-hand diagram shows average values hour by hour.

6.3. Adding Counters

Counters can be added to the diagram by right-clicking on the counter and choose **Add Counters...** from the context menu, or by selecting **Add Counters...** from the **Edit** menu which will bring up the same window.

A dialog similar to the one below will come up, with all configured gateways. Select a gateway and counters that are to be monitored. See section *Real-time Monitoring Counters* in the *CorePlus Administration Guide* for detailed information about each counter category.
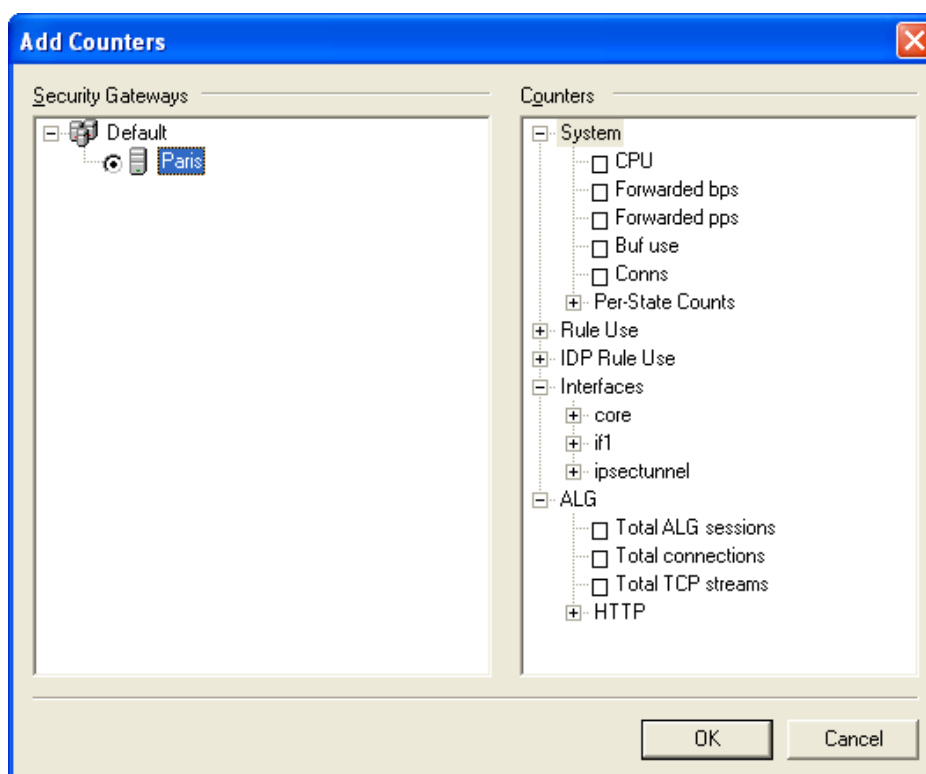
6.4. Removing Counters

To remove a monitored counter from the Real-time monitor, make it active by left clicking on the row and choose either **Remove Counter** from the **Edit** menu or by right-clicking on the counter and choose **Remove Counter** from the context menu. It is also possible to remove counters from the **Data** tab in the Real-time Monitor Properties dialog.
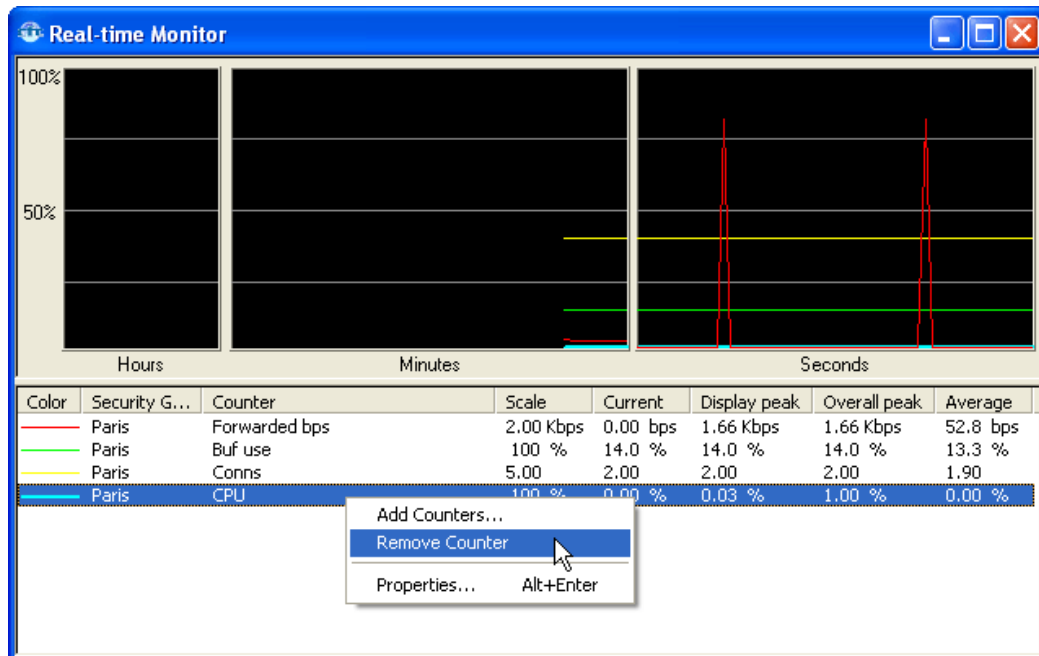
6.5. Real-time Monitor Properties

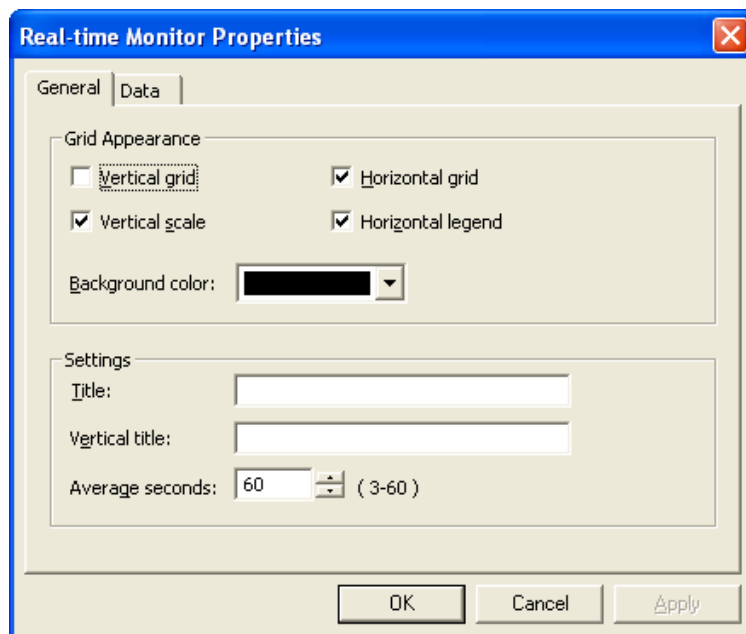To change the behaviour and look of the Real-time Monitor either choose **Properties...** from the **File** menu or by right-clicking on the counter and choose **Properties...** from the context menu, this will bring up the following dialog.

The **General** tab contains the following settings:

Grid Appearance

Vertical grid	Enables or disables the vertical grid in the diagram section.
Horizontal grid	Enables or disables the horizontal grid in the diagram section.
Vertical scale	Enables or disables the vertical scale.
Horizontal legend	Enable or disable the Hours, Minutes and Seconds legend.
Background color	Sets the color of the diagram.

Settings

Title	Specifies what if any title should be put over the diagram.
Vertical title	Specifies what if any text should be printed to the left of the vertical scale.
Average seconds	Specifies how many seconds of data which is used when calculating the average for each counter.

In the **Data** tab it is possible to add and remove counters, and change color and/or style of a plotted counter.
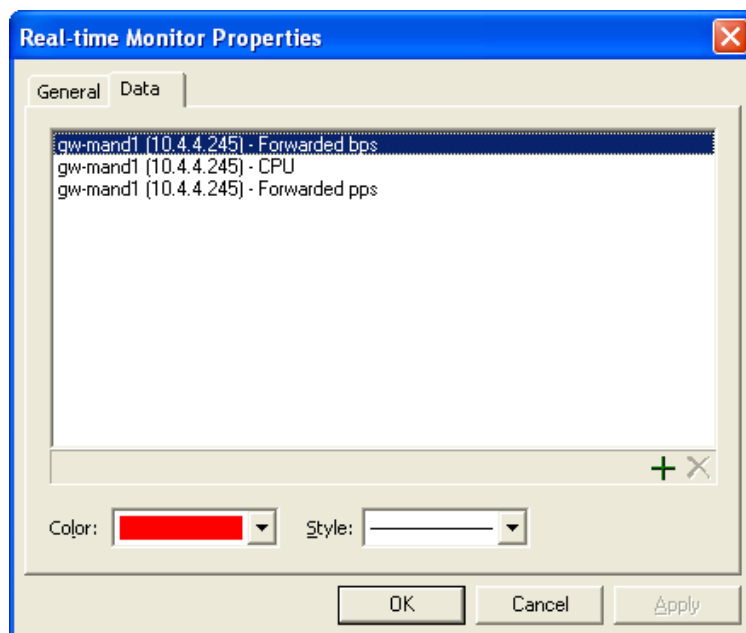
To change the color or style of a counter, first select the counter then choose what color and style it should use. Adding more counters to the list is done by clicking the button illustrated with a green plus sign. For more information about adding counters, please see Section 6.3, "Adding Counters".

To remove counters from the list, first select the counters to be removed. Press and hold the Ctrl or Shift key while selecting to include multiple items in the selection. Click the button illustrated with a red X. The selected counters will now be removed.

6.6. Real-time Monitor Templates

It is possible to save the diagram layout and added counters for faster use of Real-time Monitor. This is done by choosing **Save As...** from the **File** menu, this will let you save a .rtm file. It is then possible to open that .rtm file by choosing **Open** in the **File** menu and get the same counters and layout as when it was saved.

This is very useful when monitoring the same counters from one or more gateways every time Fine-Tune is used, as it is not convenient to add all counters every time the Real-time Monitor is started.

Note
FineTune must have access to the same gateways with same names as when the save was done in order for this to work.

Chapter 7. Remote Console

This chapter describes the Remote Console feature, which is used to access the CLI in CorePlus from within the FineTune environment.

The Remote Console sessions are encrypted using the NetCon protocol. To open the Remote Console, right-click a gateway in the **Security Editor** and choose **Remote Console** from the context menu. The **Remote Console** can also be accessed using the Remote Console icon in the left-hand **Tools** toolbar. In the latter case, a dialog box is displayed for selecting the target system.

Figure 7.1. Remote Console
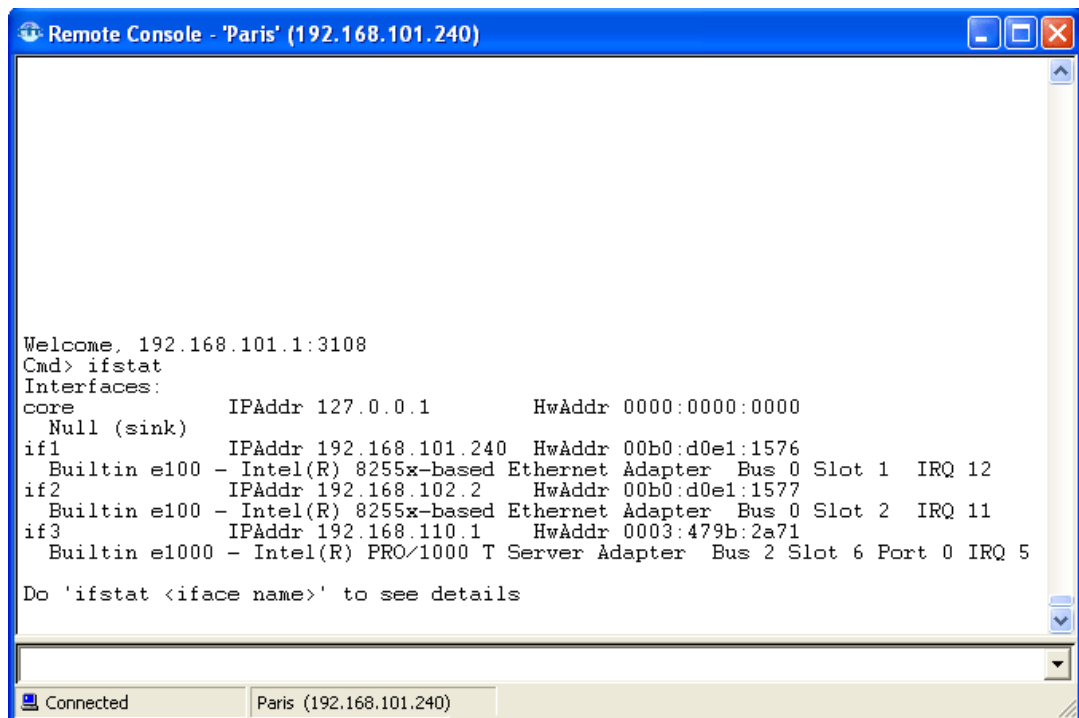
Administrators with **Configure** or **Console** rights can use this console via the network through Fine-Tune.

Appendix A. Troubleshooting a new gateway

If the New Security Gateway Wizard fails to finalize the configuration, communication with the hardware will not work as intended. One of the following may locate the problem:

Check IP addresses

Make sure you have set up the correct IP addresses and netmask.

Check FineTune communication isn't blocked

Make sure another device in the network isn't blocking UDP port 999 or TCP port 999. These are used by FineTune to communicate with the Clavister Security Gateway.

Check connections with Ping

- Try pinging the gateway from your management workstation.

- Try pinging a host on the management network from the local console on the gateway by using the serial cable.

Management interface improperly connected

- Check the link indicators of the network interface you have selected as the management interface. If there is no link indication, there might be a cable problem.

- Is your Clavister Security Gateway directly connected to a router or another host? In this case, you will need an "X-ethernet" cable to connect the gateway to that unit. Using the wrong cable type may result in the link indicators indicating link failure.

Routing problems

- If the Clavister Security Gateway and the management workstation are connected via a router, is the default gateway setting correct on both the Clavister Security Gateway and the management workstation?

It's still not working!

Should none of the above be of any assistance, check the statistics information for the management interface using the **ifstat** command. Issue the following command on the Clavister Security Gateway console:

```
> ifstat ifN
```

This will display a number of counters for the network interface. If the **Input** counters of the hardware section are not increasing, the error is likely to be in the cables. However, it may simply be the case that the packets aren't getting to the Clavister Security Gateway in the first place. You may want to verify this with a packet sniffer attached to the network in question.

If the **Input** counters of both sections are increasing, the interfaces may be attached to the wrong physical networks. Additionally, there may be a problem with the routing information in the connected hosts or routers.

Another test can be performed by running the command **arpsnoop** on the Clavister Security Gateway console. It will dump ARP packets heard on selected interfaces. Arpsnoop is a convenient method of verifying that the correct cables are attached to the correct interfaces.

```
> arpsnoop all

        ARP snooping active on interfaces: if1 if2 if3 if4
        ARP on if2: gw-world requesting ip_if2
        ARP on if1: 192.168.1.5 requesting ip_if1
```

Clavister Glossary

Clavister Hardware Series	The series of Clavister hardware appliances that run the CorePlus operating system. These include the SG50, SG3100, SG4200, SG4400 and SG5500.
Clavister Security Gateway	A hardware device which is running the CorePlus operating system.
Clavister Software Series	Versions of the CorePlus operating system which run on non-Clavister hardware.
CorePlus	A Clavister proprietary software operating system which performs all the functions of a Security Gateway.
FineTune	A proprietary Clavister software application that runs on a separate workstation to control one or many Clavister Security Gateways.
Gateway	A shortened name for a Clavister Security Gateway. In some contexts, such as VPN, this may refer to any routing device.
Firewall	Usually a hardware device which offers basic protection against unauthorized IP based security attack by monitoring the types of links established. Some firewalls are implemented in software only and run on the computing asset that they protect.
Firewalling	The function fullfilled by a Firewall. This function is a subset of the functions of a Security Gateway.
Security gateway	A hardware device which intercepts, monitors and routes IP traffic in order to prevent security attacks against particular computing assets.
SG50	A low-end Clavister hardware device that runs CorePlus, designed for small business and branch office use.
SG3100	A low to mid-range Clavister hardware device that runs CorePlus, designed for small to medium business users.
SG4200	A mid to high-range Clavister hardware device that runs CorePlus, designed for medium to large business users.
SG4400	A high-end Clavister hardware device that runs CorePlus, designed for large business users.
SG5500	A high-end Clavister hardware device that runs CorePlus, designed for telecom applications such as UMA/GAN configurations.